基于神经网络的定向口令猜测研究

周 环[1,2], 刘奇旭[1,2], 崔 翔[1,3], 张方娇[1,2]

[1] 中国科学院信息工程研究所 北京 中国 100093
[2] 中国科学院大学网络空间安全学院 北京 中国 100049
[3] 广州大学网络空间先进技术研究院 广州 中国 510006

摘要 文本口令是现如今最主要的身份认证方式之一, 很多用户为了方便记忆在构造口令时使用个人信息。然而, 目前利用用户个人信息进行定向口令猜测, 进而评估口令安全的工作相对欠缺。同时, 神经网络在文本序列处理问题上的成功应用, 使得利用神经网络进行口令安全问题研究成为一种新的研究思路。本文基于大规模口令集合, 对用户口令构造行为进行分析的基础上, 研究用户个人信息在口令构造中的作用, 进而提出一种结合神经网络和用户个人信息的定向口令猜测模型 TPGXNN(Targeted Password Guessing using X Neural Networks), 并在 8 组共计 7000 万条口令数据上进行定向口令猜测实验。实验结果显示, 在各组定向口令猜测实验中, TPGXNN 模型的猜测成功率均比概率上下文无关文法、马尔科夫模型等传统模型更高, 表明了 TPGXNN 模型的有效性。

关键词 用户个人信息; 口令安全; 定向口令猜测; 神经网络
中图法分类号 TP309.2 **DOI 号** 10.19363/J.cnki.cn10-1380/tn.2018.09.03

Research on Targeted Password Guessing Using Neural Networks

ZHOU Huan[1,2], LIU Qixu[1,2], CUI Xiang[1,3], ZHANG Fangjiao[1,2]

[1]Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[2]School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China
[3]Cyberspace Institute of Advanced Technology, Guangzhou University, Guangzhou 510006, China

Abstract Text-based passwords is one of the most important mechanisms of identity authentication nowadays. Many users tend to use personal information when constructing passwords for convenience. However, there are few studies about targeted password guessing using personal information in the field of password security. Besides, the successful application of neural network on the issue of text sequence processing makes the study of password security by using neural network become a new research idea. Based on the analysis of user's behaviors when constructing password, this thesis studies the role of user's personal information in password structure, and proposes a brand new model called TPGXNN (Targeted Password Guessing using X Neural Networks) which combines neural network and user's personal information. An experiment is carried out on 70 million password datasets. TPGXNN is compared with the current common guessing probability model including probability context-free grammar and various Markov models using guessing success rate. Experimental results show that TPGXNN model in each group of the experiments has a higher rate than the traditional password guessing model. The results not only demonstrate the validity of TPGXNN model, but also prove that the binding of neural network and user's personal information in password guessing is a practical research idea.
Key words personal information; password security; targeted password guessing; neural networks

1 引言

在身份认证中, 口令一直被认为是安全性最薄弱的一环, 所以很多人认为文本口令已经过时, 并提出了各种各样替代性的身份认证方案(如图形认证[1]、生物认证[2]、多因子认证[3]等), 但是目前仍没有任何一种替代性方案能像文本口令一样部署简单且方便使用。文本口令依然是目前最主要的身份认证方式, 并且在可预见的未来, 其在身份认证领域将继续扮演至关重要的角色[4]。

通讯作者: 刘奇旭, 博士, 副研究员, Email: liuqixu@iie.ac.cn。
本课题得到国家重点研发计划(No. 2016YFB0801604)、院重基金(No. CXJJ-17S0490)资助。
收稿日期: 2017-06-20; 修改日期: 2018-01-25; 定稿日期: 2018-08-20

在构造口令的过程中对不同的服务使用不同的随机字符序列被认为是相对安全的口令构造行为, 但是为了方便记忆力, 用户在构造口令时通常远远无法满足随机构造的要求[5-9]。通常情况下, 人们会选择对自身来说容易记忆的口令, 造成大量的口令在整个口令区间中呈现集中分布的情况, 这一现象大大提升了攻击者破解口令的成功率。

为了提升口令的安全等级, 在线的身份认证系统开始强制用户使用越来越严格的口令构造策略。同时, 很多网站部署口令强度评测器来帮助用户构造更安全的口令。然而这些口令强度评测器已经被证明是启发式的而且可持续性不强[10-11]。为了更好地评估口令的强度, 我们需要更深入地理解用户是如何构造口令的。

与最开始采用启发式的方式研究口令安全不同, 为了更加系统地研究口令安全, 近年来学术界逐渐提出一些新的口令概率模型, 比如 N 阶马尔科夫模型(Markov N-grams)[12-13]、概率上下文无关文法模型(Probabilistic Context Free Grammar, PCFG)[14-15], 这些模型及相关理论的提出将口令研究带入了一个新的研究阶段。虽然这些口令概率模型在适用范围和破解成功率上比传统的启发式的口令猜测方式更好, 但是它们在评估口令强度时忽略了用户在构造口令时的一些行为特征(如口令重用、使用个人信息), 同时由于采用统计计算的方式评估口令强度, 在实际破解过程中通常需要大量的计算资源和存储空间且运行耗时严重。因此这些口令概率模型在实际的在线口令强度评估中可用性不高。

为了更好地理解用户的口令构造行为, 同时针对传统的口令概率模型存在的问题, 我们首先在大规模口令数据集上对用户的口令构造特征进行了分析, 接着提出了一种结合人工神经网络(Artificial Neural Networks, ANN)和用户个人信息(Personal Information, PI)的定向口令猜测模型。神经网络是一种机器学习的方法, 它试图通过模拟人类大脑处理和记忆信息的方式实现信息的处理。相关研究已经表明神经网络在序列生成和处理上取得了非常成功的应用[16-17]。

本文在近年来国内外泄露的八个大规模用户口令数据集上进行了口令安全相关实验。我们首先对用户口令行为进行了分析, 发现了用户在构造口令过程中的一些行为特征。之后, 为了衡量用户个人信息与其构造口令的关联性, 我们对各个数据集中各种不同类型的个人信息进行了统计分析, 对用户在口令构造中使用个人信息这一特征进行了深入的研究, 设计了一种新的评估用户个人信息与口令之间关联度的方法 Relevance。最后为了更加准确有效地评估文本口令强度, 我们提出了一种结合神经网络和用户个人信息进行定向口令猜测的模型 TPGXNN (Targeted Password Guessing using X Neural Networks), 并将该模与传统的口令概率模型的猜测成功率进行了比较, 验证了该模型的有效性。

本文第 1 节介绍了研究的背景以及主要的研究内容; 第 2 节介绍相关工作, 包括口令猜测攻击、口令强度评估以及神经网络; 第 3 节主要通过对从公开渠道收集的大规模用户口令的实验, 分析用户的口令构造行为; 第 4 节提出了结合用户个人信息和神经网络进行定向口令猜测的模型 TPGXNN; 第 5 节在数据集上进行实验, 并将 TPGXNN 与传统的口令猜测模型进行比较; 最后, 第 6 节对本文进行总结和展望。

2 相关工作

2.1 口令强度评估

通常情况下, 口令的安全性能被划分为两大类[18-19]: 第一类是整个口令集的安全性; 第二类是单独某个口令的安全性。我们能使用攻击算法模拟现实攻击[20-22]或者使用依托于统计学的评定指标(比如香农熵[23-24]或者其他高级的统计学方法)来衡量第一类的安全性; 而第二类的安全性则只可以采用攻击算法模拟现实攻击的方式, 再通过攻击结果来进行评定。目前成功破解某一口令所实际需要的猜测次数是最常使用的评估指标。

我们基于神经网络的定向口令猜测模型便采用模拟现实口令猜测攻击的方式来验证模型的有效性。接下来, 我们简单介绍在学术界已经被广泛研究和使用的两种口令概率模型: 基于马尔科夫模型的口令概率模型(以下简称为“Markov”模型)和基于上下文无关文法的口令概率模型(以下简称为“PCFG”模型)。本文第 5 小节我们将对以上两种传统的口令猜测模型与 TPGXNN 模型的口令猜测结果进行对比。

Markov 模型 Narayanan 和 Shmatikov 于 2005 年首次提出使用 Markov 模型进行口令猜测[25]。近几年, 出现了一些更加深入系统地利用 Markov 模型进行口令安全研究的成果[26-27]。此模型假设用户在构造口令时是按一定顺序(从前到后)构造的, 基于口令前后字符之间的关联性通过统计计算的方法得到目标口令所对应的概率值。该模型在进行模拟口令猜测攻击时可以分为两个阶段: 在训练集上训练阶段

和在测试集上测试阶段。

首先, 在训练集训练阶段需要统计训练集口令中每个子串之后紧跟的那个字符频数。阶(gram)是Markov 模型的一个重要概念, N 阶 Markov 模型需统计长度为 N 的子串之后紧跟的字符频数。比如在四阶 Markov 模型中, 口令 Lin678 需统计的值有: 首字符是 L 的频数、L 后是字符 i 的频数、Li 后是字符 n 的频数、Lin 后是数字 6 的频数、Lin6 后是数字 7 的频数以及 in67 后是数字 8 的频数。按照这种方式, 每个口令经过 N 阶 Markov 模型训练之后便会得到一个概率值, 也就是从前到后将长度为 N 的子字符串在训练结果中查询, 最后把得到的所有的概率值相乘便可得到目标口令的概率值。在四阶 Markov 模型下, 口令 Lin678 的概率计算为: P(Lin678)=P(L)×P(i|L)×P(n|Li)×P(6|Lin)×P(7|Lin6)×P(8|in67)。

在测试集测试阶段, 先基于上述方法得到每个口令的概率, 按照从高到低的顺序排列就可以得到一个概率递减的猜测集。然后再用得到的猜测集对测试口令集进行破解测试即可。

PCFG 模型 Weir 等人于 2009 年提出了一个基于概率上下文无关文法进行口令概率猜测的模型[28]。PCFG 模型的核心思想是将口令按数字(D)、字母(L)以及特殊字符(S)进行分段, 并对每个段的长度进行计数表示。比如对于口令“lin&6789”, PCFG 模型将其表示成 L3S1D4, 这被称为此口令的模式。该模型在进行模拟口令猜测攻击时也可以分为在训练集训上训练和在测试集上测试两个阶段。

在训练集训练阶段最关键的是通过统计计算得到各种口令模式对应的频率以及各字符组件所对应的频率。若要得到“lin&6789”的概率值, 首先需统计在所有口令中以 L3S1D4 作为模式的口令频率, 以及“lin”在长度为 3 的字母串(L3)中的频率, “&”在长度为 1 的特殊符号(S1)中的频率, “6789”在长度为 4 的数字串(D4)中的频率。假设 P(S→L3S1D4)=0.2, P(L3→lin)=0.3, P(S1→&)=0.1, P(D4→6789)=0.2, 则口令“lin&6789”的猜测概率为: P(lin!6789) = P(S→L3S1D4)×P(L3→lin)×P(S1→!)×P(D4→6789)=0.0012, 这表明“lin&6789”的可猜测度为 0.0012。

同样的, 通过这种方法就可以计算每个口令的概率值, 按照从高到低的顺序排列就可以得到一个概率递减的猜测集。然后在测试集测试阶段使用得到的猜测集对测试口令集进行破解测试便可以评估模型在特定测试集上的口令破解的成功率。

2.2 人工神经网络

人工神经网络[29-32](Artificial Neural Network, ANN)或者被称为连接系统是由动物大脑的生物神经网络启发而设计实现的计算系统。这类系统通过样本学习(逐渐改善性能)来完成任务, 而并非通过基于特定任务的格式化编程来实现目标。例如, 在图像识别中, 神经网络可以通过对标注了“cat”和“no cat”标签的样本图片的学习来识别未标注图片中的猫。神经网络已经在很难用传统算法编程实现的领域中得到了广泛应用。

神经网络是由连接在一起的被称为神经元的节点(类似于生物脑中的轴突)所构成, 每个节点代表了一种特定的被称为激活函数(activation function)[33-35]的输出函数, 神经元之间的连接可以传递随连接强度而变化的单向信号。如果组合的输入信号(来自潜在的许多发射神经元)足够强, 则接收神经元会激活并传播一个信号到与其相连的下游神经元。

通常, 神经元被分层组织。信号从第一(输入)到最后(输出), 可能会在层与层之间遍历多次。除了接收和发送信号之外, 节点可以具有由实数表示的状态, 值通常在 0 到 1 之间。阈值或限制功能可以管理每个连接和神经元, 使得信号在传播之前必须超过特定值。

神经网络方法的最初目标是以与人类大脑相同的方式解决问题。时至今日, 其已被用于各种任务, 包括计算机视觉, 语音识别, 机器翻译, 社交网络过滤, 医疗诊断等许多领域。

2.2.1 神经网络特性

人工神经网络是由很多神经元节点相互连接组成的自适应、非线性的处理系统。在当代神经科学研究的基础之上, 人工神经网络想要通过模拟动物大脑生物神经网络处理以及记忆信息的方式来实现信息的处理[36-37]。其具备 4 个主要特性:

(1) **非线性** 在自然界中非线性关系是一种普遍特性。人工神经元有两种状态: 激活态和抑制态。在数学上, 这种行为便表现为一种非线性关系。

(2) **非局限性** 单个神经网络一般由很多神经元节点连接构成。系统的整体行为特征由两个因素决定, 一个是单个神经元的特征, 另一个是节点彼此之间的作用以及连接。神经网络通过节点间的大量连接来模拟大脑的非局限性。

(3) **非常定性** 自适应、自学习、自组织是人工神经网络具备的三种能力。神经网络不仅处理的信息能够存在很多变化, 同时在处理信息过程中, 非线性动力系统本身也在不断的变化[38]。

(4) **非凸性** 在一定条件下特定系统的演进方向将取决于某个特定的状态函数。非凸性代表这种函

数有多个极值, 所以系统存在多个较稳定的平衡态, 这会使系统系统演化存在多样性[39]。

2.2.2 循环神经网络

RNN[40-42](Recurrent neural Network, 循环神经网络)是人造神经网络的一种, 其中单元之间的连接形成定向循环。这创建了网络的内部状态, 允许其呈现动态时间行为。与前馈神经网络不同, RNN 可以使用其内部存储器来处理任意输入序列。这使得它们适用于诸如未分段连接的手写识别、语音识别以及自然语言处理[43-45](Natural Language Processing, NLP)等任务。

在 RNN 中, LSTM[46-48](Long Short-Term Memory, 长短时记忆模型)模型是现在使用范围最广也是应用最成功的模型, LSTM 能够很好地对长短时依赖进行表达, 它和一般的循环神经网络在结构本质上并没有什么本质不同, 在隐藏层的状态的计算上只是使用了不同的函数。LSTM 是一个深度学习系统, 它不存在梯度消失问题。

在传统的神经网络模型中, 输入层到隐藏层是全连接的, 隐藏层到输出层也是全连接的, 每层内部的节点之间是没有连接的。但在很多问题的处理上传统的神经网络无法很好地解决问题。比如, 判断一个未完成的句子中下一个词是什么, 需要使用句子中已有的词, 因为句子中词语之间是由联系的, 而并不是彼此孤立的。使用 RNN 便可以使一个序列当前的输出与之前的输入相关。具体的实现方式是循环神经网络存储已有的信息并将其用于当前输出的计算中, 也就是说隐藏层内部的节点之间不再是没有连接的, 相反其节点之间存在连接, 不仅如此, 在输入上, 隐藏层不仅包含输入层的输出还包含上一时刻隐藏层的输出。理论上, RNN 能够对任何长度的序列数据进行处理[47]。但在实际使用过程中, 为了降低复杂性通常假设当前的输出只与前面的几个状态存在关系, 如图 1 所示, 展示了一个典型的 RNN 结构。综合 RNN 的特点以及文本口令猜测的场景, RNN 在口令猜测上可能会得到较好的应用。本文基于 RNN 对大规模用户口令进行分析和研究, 提出了一种新的口令概率模型。

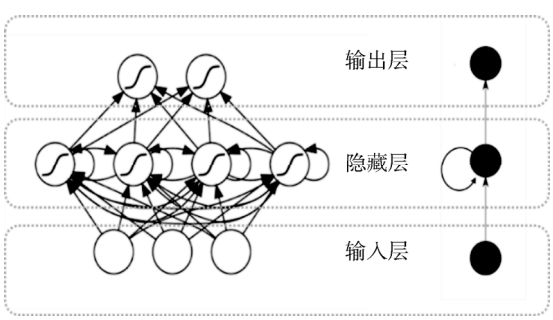


图 1 典型的循环神经网络

Figure 1 Typical Recurrent Neural Network

3 用户口令行为分析

3.1 数据集准备

口令达不到理想强度的最直接原因是用户不安全的口令行为, 所以理解用户可能存在哪些不安全的脆弱口令行为是研究口令安全性的前提条件。通常情况下用户需要管理几十个乃至上百个口令账户, 各个站点的口令设置要求也往往存在很大区别。不仅如此, 用户用于处理信息安全问题的精力有限且基本稳定。这些问题导致了用户的一系列口令行为。

本节从流行口令分析、口令重用和基于个人信息的口令构造三个方面, 对用户的常见口令行为进行了研究。我们选择了 8 个国内外数据质量较好的数据集进行口令分析和研究, 其中包括 4 个国内用户泄露数据集和 4 个国外用户泄露数集, 这些泄露的数据集均通过公开网络渠道获取, 且数据集中包含用户明文口令。表 1 中列举了这 8 个数据集的基本信息, 包括: 数据集来源、泄露网站类型、泄露数据条数、用户使用语言、数据集中是否包含用户个人信息以及数据的泄露时间。

表 1 数据集基本信息

Table 1 Data Set Basic Information

数据集来源	网站类型	泄露条数	用户语言	个人信息	泄露时间
NetEase	互联网	234,842,089	中文	×	Oct., 2015
Tianya	社区论坛	29,020,808	中文	×	Dec., 2011
GFAN	安卓论坛	22,526,334	中文	×	Oct., 2016
12306	铁路服务	129,303	中文	√	Dec., 2014
Linkedin	社交猎聘	1,000,000	英文	×	May, 2016
Yahoo	互联网	453,427	英文	×	July, 2012
Fling	社交类	40,767,652	英文	√	2011
Neopets	游戏类	26,892,897	英文	√	May, 2016

(LinkedIn大规模泄露口令被哈希加密, 我们使用从中破解的100万纯文本口令用于口令安全研究)

3.2 流行口令分析

Morris 和 Thompson 在 1979 年分析了 3289 个真实的用户口令, 发现其中有 86%的数据落入普通字典, 33%的数据能在 5 分钟内搜索出来。后续的大量研究也表明, 除了选择常用单词作为口令, 用户常常将单词做一些简单的变换, 以满足站点口令设置策略的需求。如“password1314”可以满足“字母+

数字”的策略需求。一些最常用的单词、数字、字符序列和其变换就成了大多数用户可能选择的弱口令。我们对上述 8 个数据集中最常用的口令进行了分析, 如表 2 所示。

表 2 数据集中最流行的前 10 个口令分析

Table 2 Analysis of Top 10 Most Popular Password in the Data Set

口令排名	NetEase	Tianya	GFAN	12306	Linkedin	Yahoo	Fling	Neopets
1	123456	12345678	123456	123456	123456	123456	12345678	123456
2	12345678	123456789	12345678	123456789	123456789	password	123456	password
3	111111	11111111	password	111111	password	12345678	iloveyou	qwerty
4	password	woaini1314	123123	password	iloveyou	abc123	love123	asd123
5	123123	5201314	123456a	000000	1234567	123456789	abc123	pet123
6	000000	321654	5201314	123123	princess	sunshine	princess	12345678
7	123456789	1234567	111111	12345678	linkedin	welcome	password	11111111
8	5201314	000000	11111111	5201314	secret666	asd123	11111111	qwertyui
9	1234567	123456a	00000	18881888	asd123	princess	000000	qwerty123
10	woaini1314	password	000111	1234567	qwert123	qwerty	loveyou123	iloveyou
前十口令占总口令比例	2.78%	7.31%	3.34%	1.21%	2.37%	3.12%	1.54%	3.28%

表 3 国内外用户口令的字符组成结构分析/%

Table 3 Analysis of the Character Composition of Passwords at Home and Abroad/%

数据集	[a-z]	^[a-z]+$	[0-9]	^[0-9]+$	^[a-z]+[0-9]+$	[a-zA-Z]	[A-Za-z]+$	^[a-zA-Z]+[0-9]+$	^[a-zA-Z0-9]+$
NetEase	59.45	35.78	**65.66**	24.12	20.74	61.25	38.98	28.33	**91.33**
Tianya	49.36	14.32	**90.12**	41.01	27.32	42.91	10.45	28.96	**97.33**
GFAN	66.12	11.35	**88.74**	30.41	41.54	68.14	10.41	45.68	**98.35**
12306	71.15	5.31	**93.47**	26.42	49.52	75.65	5.14	51.78	**99.14**
Linkedin	**80.41**	39.25	59.68	15.23	27.56	81.42	41.21	36.41	**96.25**
Yahoo	**84.25**	33.56	69.86	5.26	38.21	86.27	33.25	46.24	**94.31**
Fling	**90.33**	40.12	51.21	14.21	41.73	74.25	20.14	52.38	**95.34**
Neopets	**81.63**	33.41	63.27	18.74	45.21	63.25	45.96	57.43	**98.56**

表 4 用户口令长度分布分析

Table 4 Analysis of Length Distribution of Password

长度	1-5	6	7	8	9	10	11	12	13	14	≥15
NetEase	0.00	**25.12**	**20.36**	**24.34**	12.13	8.36	4.64	2.65	0.87	0.54	0.99
Tianya	1.37	**23.45**	**16.27**	**28.41**	9.45	8.32	5.76	3.52	2.15	1.34	1.33
GFAN	2.14	**15.24**	**18.63**	**32.14**	10.42	8.69	6.52	4.29	1.29	0.34	2.44
12306	3.54	**11.23**	**15.64**	**25.37**	23.16	17.65	3.64	1.59	0.47	0.32	0.93
Linkedin	1.94	**29.63**	**15.46**	**19.95**	12.69	9.43	3.57	2.10	1.36	0.84	4.97
Yahoo	2.65	**26.12**	**18.63**	**27.14**	10.25	8.74	4.31	1.21	0.96	0.74	1.90
Fling	0.32	**33.14**	**16.13**	**21.73**	11.39	8.42	3.47	2.53	1.38	1.10	0.71
Neopets	2.36	**21.12**	**17.41**	**25.84**	14.13	7.62	6.58	3.14	0.72	0.27	3.17

通过对以上结果的分析, 可以发现: 1)不管是国内用户还是国外用户都倾向使用一些常见的、方便记忆(比如, 数字、字母以及键盘模式)的口令; 2)国内用户中流行使用的口令多为数字, 而国外用户使用英文字母、单词或者简单的键盘模式来构造口令居多, 这体现了语言因素对口令行为的影响; 3)爱情在国内外用户构造口令的过程中都扮演了重要角色, “iloveyou”和“princess”均出现在最流行的前 10 个口令中, 而“5201314”和“woaini1314”这种明显有地域特点与爱情相关的口令则出现在了国内用户最

流行的前 10 个口令中; 4)不仅如此, 文化以及网站名(比如“linkedin”)等因素也在用户最流行的口令中得到体现。

相对于其他口令来说, 这些流行口令在整个口令集中占的比例很高, 同时考虑到口令集庞大的基数, 可以说这些流行口令的使用规模还是非常庞大的。这意味着攻击者如果发现这一现象, 只要尝试最流行的一些口令, 就很有可能破解大量的用户账户信息。同时通过对这 8 个网站的流行口令分析, 也可以发现口令的分布远不是均匀的。

3.3 用户口令字符组成分析

大多数网站会设置口令限制条件(比如, 口令长度、字符种类等), 这种情况下口令的字符组成通常会受到口令限制条件的影响。如果网站没有设置口令构成限制条件, 用户使用的口令结构就直接反映了用户口令构造过程中使用字符类型的偏好。本文对目标数据集的口令字符组成进行了分析, 在分析中用正则表达式定义了 9 种常见模式, 并对各个数据集中相应模式的口令比例进行了统计。表 3 显示了国内外用户口令的字符组成结构。

通过对以上结果的分析, 可以发现: 1)用户会使用包含特定模式的口令, 且有一些普遍存在的用户口令构成行为。比如, 用户口令绝大多数都是由数字或字母组成, 使用纯数字或者纯字母的用户比例都比较高; 2)在国内外用户口令组成模式对比方面, 国内大多数用户会在口令中包含数字, 而国外用户则更偏爱使用字母。这一点也体现在使用纯数字作为口令的国内用户比例多于国外用户, 而使用纯字母作为口令的用户比例则国外用户更多。

用户在口令字符组成中的这些偏好正是攻击者所努力挖掘的对象, 因为使用这些用户习惯, 通过构造包含用户常用模式的口令就可以大大提升破解用户口令的效率。

3.4 用户口令长度分析

口令的长度同样直接受到网站口令设置限制条件的影响。大多数用户口令安全意识不强, 选择的口令长度往往只满足网站口令限制的最短长度要求。显然, 口令的长度大小直接影响攻击者实施口令猜测攻击的攻击范围, 下面对目标数据集中的口令长度进行了统计。表 4 显示了 8 个数据集中用户口令长度的分析结果。

通过对以上结果的分析, 可以发现: 1)用户的口令长度选择存在集中分布的特点; 2)对于普通网站来说, 长度为 6,7,8 用户口令分布最多的, 过长或者过短的口令在整个口令集合中分布都很少; 3)用户使用最多的几种口令长度与大多数网站限制的最短口令长度相近。

这一分析结果揭示了用户在口令构造中在长度选择上存在集中分布的特点, 而且跟特定站点在用户设置口令过程中限制的最短口令长度相近。这一分析结果对于攻击者在猜测攻击中减少猜测空间的大小具有重要意义。

3.5 用户口令重用分析

由于用户通常拥有几十个甚至上百个口令账户, 为了方便记忆和管理口令, 用户往往会选择在不同站点之间重复使用相同的口令。为了进一步分析用户在不同站点之间的口令重用行为, 本文基于最大共同距离 LCS 算法, 对国内和国外用户的口令重用情况进行了分析。分析过程中通过用户的邮箱将两个不同的数据集进行合并, 保存在两个数据集中都包含某一相同邮箱的记录, 从而得到一个交叉数据集, 然后在交叉数据集上测量用户口令的重用情况。本文对 NetEase&12306、GFAN&Tianya、Linkedin&Yahoo、Fling&Neopets 这四个交叉数据集中用户的直接口令重用行为和间接口令重用行为进行了分析, 其中前两个交叉数据集针对国内用户, 后两个交叉数据集则针对国外用户。表 5 显示了这四个交叉数据集中口令直接重用的比例。

图 2 则显示了这四个交叉数据集除去直接口令重用的记录后, 不完全相同口令的 LCS 分析结果, 即用户口令间接重用的结果。

表 5 交叉数据集中口令直接重用比例分析

Table 5 Analysis of proportion of Password Direct Reuse in Cross Data Sets

交叉数据集	数据条数	口令直接重用比例
NetEase&12306	3,434	55.64%
GFAN&Tianya	23,659	63.12%
Linkedin&Yahoo	4,073	44.31%
Fling&Neopets	52,346	40.78%

通过结果的分析, 可以发现: 1)口令重用在国内外用户中都是一种普遍存在的现象; 2)用户在不同站点之间直接重用口令的概率很高, 与国内用户相比, 国外用户直接重用口令的比例相对较低; 3)在间接重用口令方面, 国外用户间接重用口令的相似度更小, 约 40%左右间接重用的中文口令相似度在[0.6,1], 国外用户只有 25%左右。

一直以来口令重用行为被认为是不安全的, 因此用户应尽可能地避免不同站点之间口令的大量重用行为。

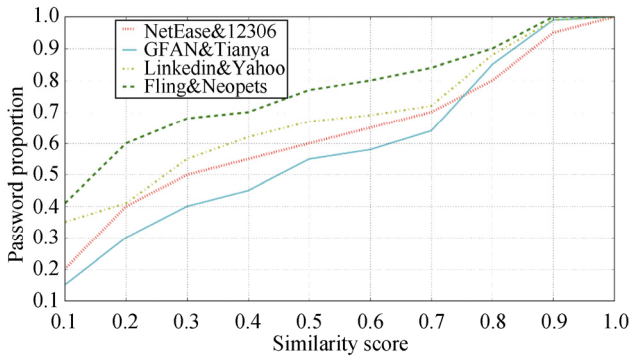


图 2 不同数据集口令间接重用分析

Figure 2 Analysis of Indirect Reuse Password in Different Data Sets

4 TPGXNN

4.1 基于个人信息的用户口令构造分析

口令攻击可分为漫步口令攻击和定向口令攻击两种, 这两者之间最突出的不同点在于在攻击过程中是否使用用户的个人信息(PI, Personal Information)。个人信息大多数情况下可以和用户可识别信息(PII, Personal Identifiable Information)交替使用。通常情况下, 一个用户的个人信息是指与这个用户相关的任何信息, 它的含义比用户可识别信息更加广泛。对于部分数据集中不包含用户个人信息情况, 我们采用了与口令重用分析中相似的方式, 将包含个人信息的数据集与不包含个人信息的数据集通过邮箱匹配的方式进行关联, 从而达到给数据集中记录添加个人信息的目的。为了尽可能多的增加表 1 数据集中包含个人信息的记录条数, 我们选择了四个用于补充用户个人信息的数据集。如表 6 所示。

表 6 补充数据集

Table 6 Supplementary Data Set

数据集	泄露条数	语言	个人信息种类
Hotel	20,051,426	中文	Name,Sex,Birth,NID
51job	2,327,571	中文	Name,Sex,Birth,Phone
ClixSense	2,424,784	英文	Name,Sex,Birth,IP,Addr
Experian	7,196,890	英文	Name,Sex,Birth,IP,Addr,Phone

在对数据集进行关联之后, 从表 1 中不包含用户个人信息的数据集中提取了关联后的数据子集, 并进行了基于个人信息的口令构造分析。具体分析结果如表 7 所示, 表中数据代表包含特定种类用户个人信息的口令在总的口令中所占的比例。

表 7 中的统计数据显示了各种类型的用户个人信息与用户口令之间的关联性, 但是却无法准确地、数值化地衡量用户个人信息在单独某个口令构造中所起的作用。所以, 我们提出了一种可以准确系统地衡量用户个人信息在口令构造中所造成影响的方法——Relevance。

Relevance 方法的值域为[0,1], 值越大说明用户个人信息在口令构造中所起的影响越大, 值为 0 说明没有影响, 值为 1 说明整个口令是由单一某种个人信息构成。Relevance 的值反映了单一口令中用户个人信息所造成的影响, 其在某个集合上的均值则能反映这个集合上用户个人信息与口令之间的关联性。

为了计算 Relevance 的值, 我们将口令和用户个人信息作为字符串输入并且使用一个滑动窗口来进行计算。通过维护一个动态窗口从口令的头部滑到尾部。窗口的初始大小为 2, 如果窗口覆盖的子串匹配了某种个人信息, 就将窗口大小增加 1, 然后尝试在更大的窗口中匹配个人信息。如果发现匹配, 则进一步扩大窗口大小直到发现不匹配。发现不匹配后将窗口大小重置为 2, 然后从不匹配的位置重新开始滑动窗口。同时我们维护了一个与口令长度相同的标记字符串, 用来记录每个匹配用户个人信息的口令子段的长度。在完成对目标口令从头到尾整个滑动过程之后, 标记字符串中记录的值便用来计算 Relevance 的值。计算公式如下:

$$\text{Relevance} = \log_2\left(1+\sum_{i=1}^{n}\frac{\text{len}_i^{\,3}}{\text{len}_{\text{total}}^{\,3}}\right) \tag{1}$$

式(1)中 n 代表了匹配的口令子串数, len_i 代表了匹配的口令子串的长度, $\text{len}_{\text{total}}$ 则代表整个口令的长度。比如对于出生于 1988 年 3 月 14 日, 名叫 Curry 的用户的口令是“curry314@@”, 在完成窗口滑动之后, 标记字符串为 [5,5,5,5,5,3,3,3,0,0], 字符串中前五个元素 {5,5,5,5,5} 代表了口令中的前五个元素匹配了特定种类的个人信息(本例中是姓名), 紧跟的三个元素 {3,3,3} 代表了口令中接下来的 3 个字符也匹配用户个人信息(本例中是生日), 最后的两个元素 {0,0} 则说明口令的最后两个字符不匹配用户个人信息。则相关度的计算为:

$$\text{Relevance} = \log_2\left(1+\frac{5^3+3^3}{10^3}\right) = 0.204$$

为了更准确系统地评估用户个人信息在每个数据集中所造成的影响, 我们在每个数据集上计算了 Relvance 的平均值——AvgRelevance。

通过分析结果可以发现, 跟预想的情况一致, 在构造口令过程中使用个人信息是一种普遍存在的现象, 就选择的数据集来说, 个人信息在国内用户

的口令构造中的影响要大于国外用户。用户通常喜欢在口令中包含个人信息, 特别是姓名、生日。而且在对姓名和生日进行使用的过程中, 用户还经常会对它们做相应的变化, 比如, 仅使用姓氏、仅使用名字、仅使用生日的年份、仅使用生日的日期、使用缩写等。与国外用户相比, 国内用户使用姓名和生日构造口令的比例更大, 所以相对来说国外用户的口令安全意识更强。还有一个有趣的现象是, 除了使用个人信息外, 用户的账号名和邮箱前缀也在口令构造中起到了一定作用。电话号码和身份证号在口令中出现的概率不高。而像用户住址、性别以及 IP 地址这些信息, 虽然也属于用户个人信息范畴, 但是却极少出现在用户的口令中。

这一分析结果在口令定向破解中能让在进行猜测攻击时, 更有针对性地使用用户个人信息, 提高猜测攻击的准确性。在接下来要介绍的定向口令猜测实验中我们就基于上述分析结果, 利用了用户的姓名、生日、用户名以及邮箱前缀来对模型进行训练。

表 7　基于个人信息的口令构造分析

Table 7　Analysis of Password Construction Based on Personal Information

个人信息	NetEase	Tianya	GFAN	12306	Linkedin	Yahoo	Fling	Neopets
姓名	14.32%	19.21%	10.34%	18.15%	3.41%	2.07%	4.35%	1.47%
生日	23.12%	17.93%	29.45%	24.02%	1.47%	1.85%	2.56%	0.96%
账户名	1.43%	1.07%	0.76%	1.96%	2.79%	2.83%	3.96%	2.64%
邮箱前缀	6.12%	4.36%	5.15%	3.03%	1.34%	2.47%	0.65%	3.58%
电话号码	0.84%	0.35%	0.10%	0.07%	0.24%	0.96%	1.13%	0.28%
身份证号	1.56%	1.89%	0.91%	0.46%	—	—	—	—
住址	—	—	—	—	0.00%	0.04%	0.13%	0.09%
性别	0.96%	0.07%	0.14%	0.12%	0.62%	0.58%	0.04%	0.96%
IP 地址	—	—	—	—	0.00	0.00	0.00	0.00
AvgRelevance	**0.26**	**0.31**	**0.29**	**0.35**	**0.17**	**0.13**	**0.21**	**0.18**

4.2　基于循环神经网络的定向口令猜测

本文中我们用神经网络来对口令进行建模。神经网络的设计模仿了人类的神经元, 它在模糊分类和序列生成上得到了很好的应用。文献[49]研究了从字符串中前面的字符元素序列来预测下一个字符元素的出现概率, 本文用于生成候选猜测口令的方法便是参考了相关研究成果。比如, 在字符串“password”的生成中, 如果把“passwor”作为参数输入神经网络, 那么字符“d”很有可能作为结果被输出。

虽然口令生成和文本生成在概念上很相似, 用自然语言生成的方法来研究口令生成的研究却非常少。神经网络在十年前曾经被提出用于对口令的强和弱进行划分, 但是此工作却并没有尝试对口令的可能猜测序列进行建模, 也没有对口令猜测攻击的相关方面进行研究。

与马尔科夫模型类似, 本文在给定前序字符序列的情况下, 使用训练好的神经网络来生成口令的下一个字符。图 3 对使用神经网络构造口令片段的下一个字符的过程进行了举例介绍。与马尔科夫模型一样, 神经网络需要依赖一个特殊的口令结束标记来计算一个口令序列的概率。比如, 为了计算口令“you”的概率, 首先以空口令作为开始, 然后从网络中查询第一个字符是“y”的可能性; 然后查询在“y”之后是 “o”的可能性; 接着查询“yo”之后是“u”的可能性; 最后查询在“you”之后出现结束标记的概率。

为了从神经网络模型中生成口令, 我们枚举了高于某一个给定阈值的所有口令。然后按照口令的概率值对它们进行排序, 排序后的口令作为猜测集。从根本上说, 此方法生成猜测集的方式与马尔科夫模型十分相似。但在文献[12]中利用神经网络进行漫步口令猜测却取得了比传统的马尔科夫模型更好的实验结果。

上文中对用户使用个人信息构造口令这一现象进行了实验分析, 分析结果发现用户使用个人信息构造口令是一种较为普遍的现象。

结合用户在生成口令过程中使用个人信息这一现象以及神经网络在序列生成中的有效应用。本文提出了一种基于神经网络的定向口令猜测方法——TPGXNN(Target Guess Using X Neural Networks), 并使用该方法在表 8 的数据集上进行了实验。下面分别对实验的方法和结果进行介绍。

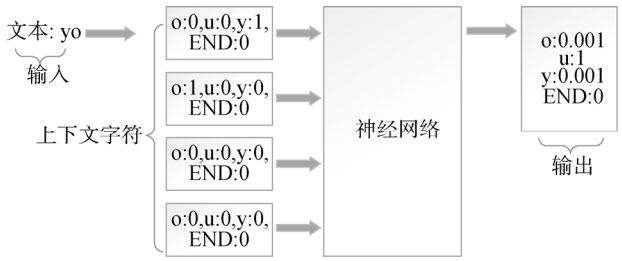


图 3 使用神经网络构造口令片段的下一个字符过程举例

Figure 3 An Example of the Construction procedure of Next Character of a Password Fragment Using a Neural Network

4.3 TPGXNN 模型结构设计与实现

神经网络包含输入层、隐含层和输出层三层，从输入层到隐含层最后到输出层。对于传统的神经网络模型，两层之间彼此采用全连接的方式传递信息，每层内部的节点之间则彼此不相连接。基于这种构造设计的神经网络在处理一些问题时无法达到预期的效果。比方说在一个预测单词序列的场景中，由于一个句子中的单词彼此之间存在关联而并不是相互独立的，所以如果想预测一个给定序列的下一个单词是什么，通常要结合序列已有的单词来进行。

不同于传统的 FNNs(Feed-forward Neural Networks，前向反馈神经网络)，RNNs(Recurrent Neural Networks，循环神经网络)引入了定向循环，能够处理那些输入之间前后关联的问题。

循环神经网路的核心设计理念是一个序列当前的输出与前面的输出存在关联。更为具体的表现形式是循环神经网络会将之前产生的信息进行记忆，然后在当前输出的计算过程中使用之前产生的信息，在其内部结构的表现上就是隐藏层之间的节点不再是无连接的，而是有连接的，而且某一时刻隐藏层的输入不但包含输入层的输出还包含上一个时刻隐藏层的输出。

相关研究已经证明循环神经网络在字符级别的自然语言生成中是非常成功的。因此本文基于目前广泛使用的一种循环神经网络模型——LSTM(Long Short-Term Memory，长短时记忆)[50]来构造 TPGXNN 模型。

在模型的构造上，模型整体由 3 层 LSTM 循环层和 2 层密集连接层构成。在服务器端基于 Keras 库完成模型的构建，实验的训练和测试阶段均使用 python 来实现。图 4 展示了模型结构。如图 4 所示，整个模型的训练包含了 3 个阶段：数据准备、训练阶段、猜测阶段。数据准备和猜测阶段的实现与传统的口令概率模型相同，模型实现的关键在于训练阶段。为了提高猜测的成功率，在训练过程中我们使用迁移学习的方法来完成模型的训练，采用这种方式，网络的不同部分在训练过程中通过学习能识别不同的现象。在使用迁移学习时，首先在整个口令集上训练口令。然后模型的低层将被锁定，最后在目标数据集上进行训练，这么做的目的是模型低层可以学习数据的低级特征(比如 e 是一个元音字母)，而模型的高层则能够学习数据的高级特征(比如元音字母通常跟在辅音字母后)。在模型大小的选择上，我们必须决定在模型中包含多少个参数，我们测试了一个包含 682,851 个参数的神经网络。

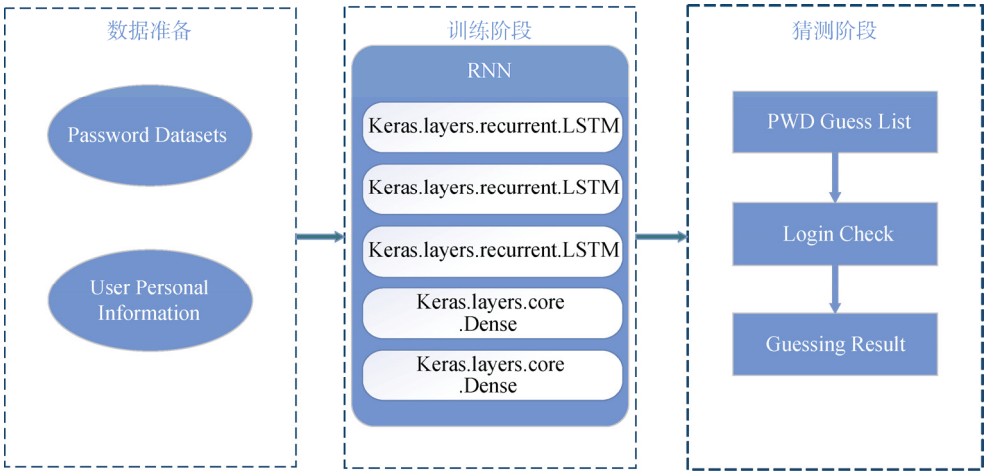


图 4 TPGXNN 模型结构

Figure 4 TPGXNN Model Structure

表 8 TPGXNN 口令猜测实验数据集

Table 8 TPGXNN Password Guessing Experimental Data Set

数据集来源	网站类型	记录条数	用户语言	个人信息	泄露时间
NetEase	互联网	289,847	中文		Oct., 2015
Tianya	社区论坛	174,356	中文		Dec., 2011
GFAN	安卓论坛	313,422	中文	姓名	Oct., 2016
12306	铁路服务	129,303	中文	生日	Dec., 2014
Linkedin	社交、猎聘	432,321	英文	用户名	May, 2016
Yahoo	互联网	1,413,212	英文	邮箱前缀	July, 2012
Fling	社交类	40,767,652	英文		2011
Neopets	游戏	26,892,897	英文		May, 2016

5 实验结果

5.1 数据集关联

为了实现定向的口令猜测, 需要准备包含用户个人信息的数据集, 如表 1 所示, 部分数据集中不包含用户个人信息。我们采用与基于个人信息的口令构造分析中相同的方法, 通过用户邮箱将包含用户个人信息的数据集和不包含用户个人信息的数据集进行关联, 得到了八个包含用户个人信息的数据集。结合上文中的分析结果, 可知并不是所有的用户个人信息在口令构造中都占有很重要的比重, 所以本文提取了用户姓名、生日、账号、邮箱前缀这四类用户个人信息并将他们加入训练过程。表 8 显示了实验过程中使用的数据集信息, 训练集包含了用户的口令信息以及提取出的四类用户个人信息。

5.2 实验环境

本文使用 Python 实现模型的训练和测试, 实验环境如表 9 所示。

表 9 实验环境参数

Table 9 Experimental Environment Parameters

属性	内容
CPU	Intel(R) Xeon(R) CPU E5
内存	64GB
操作系统	Ubuntu 14.04.4 LTS
开发语言	Python

5.3 实验结果

为了评估 TPGXNN 模型的性能, 本文在表 8 所列数据集上, 对其与现在最主流的两种传统的口令猜测模型(PCFG 模型, Markov 模型)进行了对比实验。在 PCFG 模型和 Markov 模型的训练和测试中使用与 TPGXNN 模型相同的训练集和测试集, 在训练过程中将用户个人信息看作口令加入到训练集中进行训练。由于 Markov 模型阶数的不同得到的结果也不同, 因此我们选择了阶数分别为 4 阶、3 阶和 1 阶的 Markov 模型分别进行了实验, 实验结果如图 5a-d 所示。

在实验数据集的划分上, 我们将 8 个数据集划分成 4 组进行实验。划分过程中首先按照用户的语言分为国内数据集和国外数据集, 这么做的目的是为了保证猜测模型的成功率; 然后分别将 4 个国内数据集和 4 个国外数据集随机划分成两组, 每组两个数据集。分组完成之后, 将组内的 2 个数据集其中的一个作为训练集进行训练, 将另外一个数据集当做测试集测试口令猜测的成功率, 即在给定的猜测数下数据集合中口令的破解百分比。

通过图 5 显示的实验结果可以发现, 本文提出的 TPGXNN 模型与 Markov 和 PCFG 这两种传统的口令猜测模型相比在猜测次数 10 到 10000 范围内, 其破解口令的成功率明显更高, 平均地, TPGXNN 是四阶 Markov 模型的猜测成功率的 2.65 倍, 是 PCFG 模型的猜测成功率的 2.27 倍, 这不仅说明了用户个人信息在口令猜测中确实起到了重要的作用也证明了 TPGXNN 模型的有效性。

综合上述实验结果的分析, 可以说明 TPGXNN 是一种有效的口令猜测模型, 结合神经网络和用户个人信息进行用户口令猜测是一种切实可行的研究思路。

6 总结与展望

本文首先选择了从公开渠道可获取的 8 个较有代表性国内外泄露数据集作为研究对象, 其中国内和国外泄露数据集各 4 个; 接着分别对用户口令构造的偏好性选择、用户口令重用情况以及基于个人信息的口令构造这三个方面进行了分析, 发现了口

令构造过程中存在的一些常见现象并设计了一种新的评估用户个人信息与口令之间关联性的方法

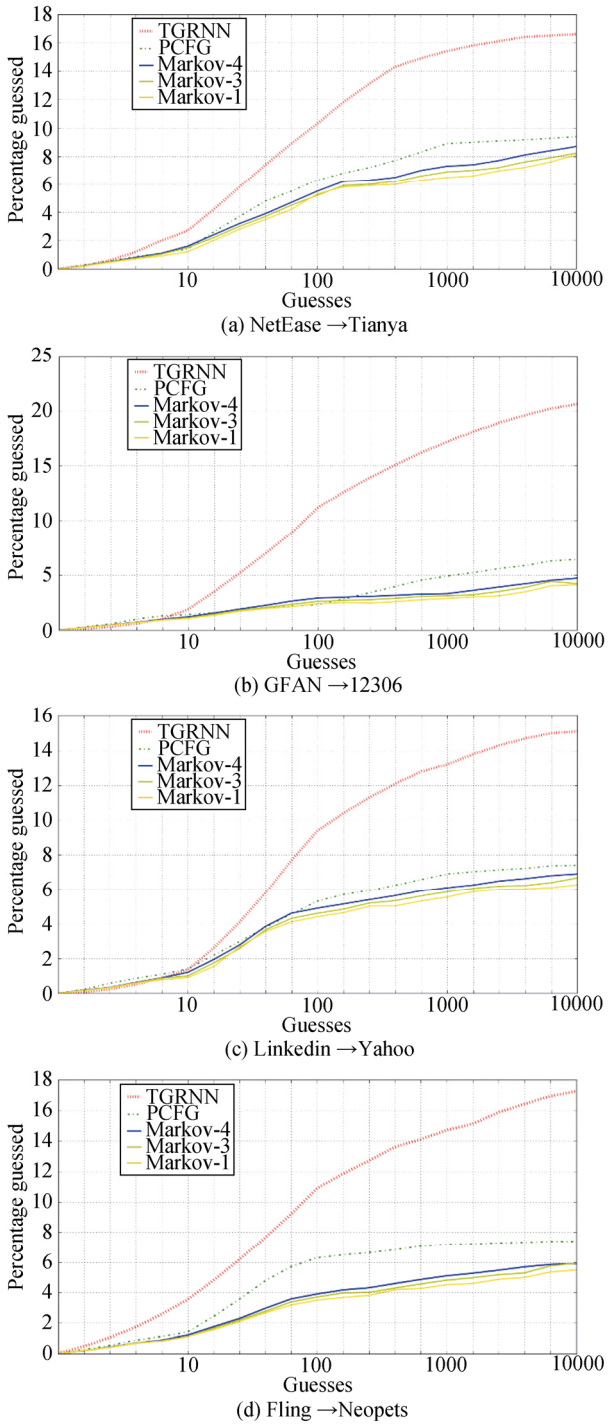


图 5 四种情况下各类口令猜测模型比较

Figure 5 Comparison of Various Types of Password Guessing Models in Four Cases

Relevance; 最后结合分析得到的结果, 提出了一种结合神经网络和用户个人信息进行定向口令猜测的方法, 设计了猜测模型——TPGXNN, 并在数据集上进行了对比实验, 对此方法和现在主流的几种口令猜测方法的猜测成功率进行了比较, 验证了模型的可行性和有效性, 对口令安全进行了有益探索。

在接下来的工作中, 我们将对利用神经网络进行口令定向猜测进行更加深入的研究, 包括模型结构和大小不同对猜测成功率的影响以及各种不同类型的神经网络在口令猜测领域的应用等。

参考文献

[1] Biddle R, Chiasson S, and Van Oorschot P C, “Graphical passwords: Learning from the first twelve years,” *ACM Computing Surveys*, vol 44(4), no. 19, 2012.

[2] Yang Y, Lu H, Liu J K, and et al, “Credential wrapping : From anonymous password authentication to anonymous biometric authentication,” *in Proc. ASIACCS 2016, New York: ACM*, pp. 141-151, 2016.

[3] Wang D, Wang N, Wang P, and et al, “Preserving privacy for free: Efficient and provably secure two-factor authentication scheme with user anonymity”. *Information Sciences*, 2015, vol. 321, pp. 162-178.

[4] Bonneau J, Herley C, Van Oorschot P C, and et al, “Passwords and the evolution of imperfect authentication,” *Communications of the ACM*, vol. 58, no.7, pp. 78-87.

[5] J. Bonneau, “The science of guessing: analyzing an anonymized corpus of 70 million passwords,” *in Proc. IEEE Symp. Security & Privacy(S&P’12)*, 2012.

[6] D. Malone and K. Maher, “Investigating the distribution of password choices,” in *ACM World Wide Web(WWW’12)*, 2012.

[7] Leonhard M D and Venkatakrishnan V N, “A comparative study of three random password generators,” *IEEE International Conference on Electro/information Technology(EIT 2007)*. pp.227-232, 2007.

[8] R. Veras, J. Thorpe, and C. Collins, “Visualizing semantics in passwords: The role of dates,” in *IEEE VizSec*, 2012.

[9] J. Yan, A. Blackwell, R. Anderson, and A. Grant, “Password memorability and security: Empirical results,” *IEEE Security & Privacy Magazine*, 2004.

[10] X. de Carne de Carnavalet and M. Mannan, “From very weak to very strong: Analyzing password-strength meters,” in Proc. *Network and Distributed System Security Symposium (NDSS’14)*, 2014.

[11] S. Egelman, A. Sotirakopoulos, I. Muslukhov, K. Be znosov, and C. Herley, “Does my password go up to eleven?: the impact of password meters on password selection,” in Proc. *the ACM SIGCHI Conference on Human Factors in Computing Systems(CHI’13)*, 2013.

[12] W. Melicher, B. Ur, S. M. Segreti, S. Komanduri, L. Bauer, N. Christin, L. F. Cranor, “Fast lean and accurate: Modeling password guessability using neural networks”, *Proceedings of USENIX Security*, 2016.

[13] Vaithyasubramanian S, and Christy A, “A scheme to create secured random password using Markov chain,” *Advances in Intelligent Systems & Computing*, vol. 325, pp. 809-814.

[14] R. Veras, C. Collins, and J. Thorpe, “On the semantic patterns of passwords and their security impact,” in Proc. *Network and Distributed System Security Symposium (NDSS’14)*, 2014.

[15] M. Weir, S. Aggarwal, B. de Medeiros, and B. Glodek, “Password cracking using probabilistic context-free grammars,” in Proc. *IEEE Symp. Security and Privacy (SP’09)*, pp. 391–405, 2009.

[16] Chung J, Gulcehre C, Cho K H, and et al, “Empirical Evaluation of Gated Recurrent Neural Networks on Sequence Modeling,” *Eprint Arxiv*, 2014.

[17] SUTSKEVER, I., MARTENS, J., AND HINTON, and G. E, “Generating text with recurrent neural networks,” in Proc. *International Conference on Machine Learning(ICML’11)*, 2011.

[18] Ma J, Yang W, Luo M, and et al, “A Study of Probabilistic Password Models,” in Proc. *IEEE Symp. Security and Privacy (SP’14)*, pp. 689-704, 2014.

[19] “Understanding passwords of Chinese users: Characteristics, security, and implications,” *ChianCrypt*, http://t.cn/RG8RacH, 2015.

[20] Wang D, Zhang Z, Wang P, and et al, “Targeted Online Password Guessing: An Underestimated Threat,” in Proc. *ACM Sigsac Conference on Computer and Communications Security(CCS ‘16)*, pp. 1242-1254, 2016.

[21] Li Y, Wang H, and Sun K, “A study of personal information in human-chosen passwords and its security implications,” in Proc. *IEEE Conference on Computer Communications(INFOCOM’16)*, pp. 1-9, 2016.

[22] VERAS, R., COLLINS, C., AND THORPE, and J, “On the semantic patterns of passwords and their security impact,” in Proc. *Network and Distributed System Security Symposium (NDSS’14)*, 2014.

[23] Singh B and Singh A P, “Edge detection in gray level images based on the shannon entropy,” *Journal of Computer Science*, vol. 4, no. 3 pp. 186-191, 2008.

[24] Wu Y, Zhou Y, Saveriades G, and et al, “Local Shannon entropy measure with statistical tests for image randomness,” *Information Sciences*, vol. 222, no. 222, pp. 323-342, 2013.

[25] Arvind Narayanan and Vitaly Shmatikov, “Fast dictionary attacks on passwords using time-space tradeoff,” in Proc. *ACM conference on Computer and communications security(CCS’05)*, 2005.

[26] Zhigong Li , Weili Han and Wenyuan Xu, “A large-scale empirical analysis of chinese web passwords,” in Proc. *USENIX conference on Security Symposium(USENIX Security’14)*, pp.559-574, 2014.

[27] Castelluccia C, Dürmuth M, and Perito D, “Adaptive password-strength meters from markov models,” in Proc. *Network and Distributed System Security Symposium (NDSS’12)*, 2012.

[28] Shiva Houshmand, Sudhir Aggarwal, and Randy Flood, “Next Gen PCFG Password Cracking,” in Proc, *IEEE Transactions on Information Forensics and Security(TIFS’15)*, pp. 1776-1791, 2015.

[29] Hsu, Kuo‐lin, Gupta H V, and Sorooshian S, “Artificial Neural Network Modeling of the Rainfall‐Runoff Process,” *Water Resources Research*, vol. 31, no. 31, pp. 2517-2530, 1995.

[30] Murata N, Yoshizawa S, and Amari S I, “Network information criterion-determining the number of hidden units for an artificial neural network model,” *IEEE Transactions on Neural Networks*, vol. 5,no. 6, pp. 865-872.

[31] Jane A P and Pund M A, “Recognition of Similar Shaped Handwritten Marathi Characters Using Artificial Neural Network,” *Science*, vol. 260, no. 5107, pp. 511-515.

[32] Gevrey M, Dimopoulos I, and Lek S, “Review and comparison of methods to study the contribution of variables in artificial neural network models,” *Ecological Modelling*, vol. 160, no. 3, pp. 249-264, 2003.

[33] Chandra P and Singh Y, “An activation function adapting training algorithm for sigmoidal feedforward networks,” *Neurocomputing*, vol. 61, no. 1, pp. 429-437, 2004.

[34] Fiori S, “Blind signal processing by the adaptive activation function neurons,” *Neural Networks*, vol. 13, no. 6, pp. 597-611, 2000.

[35] Piazza F, Uncini A, and Zenobi M, “Artificial Neural Networks With Adaptive Polynomial Activation Function,” *Handbook of Measuring System Design*, vol. 54, no. 6, pp. 36-62, 1992.

[36] Hinton G E, Srivastava N, Krizhevsky A, and et al, “Improving neural networks by preventing co-adaptation of feature detectors,” *Computer Science*, vol. 3, no. 4, pp. 212-223, 2012.

[37] Haykin S, “Neural Networks: A Comprehensive Foundation,”*Neural Networks A Comprehensive Foundation*, pp. 71-80, 1994.

[38] Schmidhuber J, “Deep Learning in neural networks: An overview,” *Neural Networks*, pp. 61:85, 2015.

[39] Nguyen A, Yosinski J, and Clune J, “Deep neural networks are easily fooled: High confidence predictions for unrecognizable images,” in Proc. *IEEE Computer Vision and Pattern Recognition(CVPR)*, pp. 427-436, 2015.

[40] Graves A, Mohamed A R, and Hinton G, “Speech recognition with deep recurrent neural networks,” vol. 38, no. 2003, pp. 6645-6649, 2003.

[41] Angeline P J, Saunders G M, and Pollack J B,” “An evolutionary algorithm that constructs recurrent neural networks,” *IEEE Transactions on Neural Networks*, vol. 5, no. 1, pp. 54, 1994.

[42] Williams G, Baxter R, He H, and et al, “A comparative study of RNN for outlier detection in data mining,” in Proc. *IEEE International Conference on Data Mining(ICDM’02)*, pp. 709-712, 2002.

[43] Kantor P, “Foundations of Statistical Natural Language Processing,” *Information Retrieval Journal*, vol. 4, no. 1, pp. 80-81, 2001.

[44] Jurafsky D, and Martin J H, “Speech and Language Processing: An Introduction to Natural Language Processing, *Computational Linguistics, and Speech Recognition*,” vol. 36, no. 23, pp. 161-187, 2000.

[45] Kumar A, Irsoy O, Ondruska P, and et al, “Ask Me Anything: Dynamic Memory Networks for Natural Language Processing,” *Computer Science*, 2015.

[46] Greff K, Srivastava R K, Koutnik J, and et al, “LSTM: A Search Space Odyssey,” *IEEE Transactions on Neural Networks & Learning Systems*, vol 99, pp, 1-11.

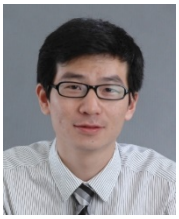
[47] Sundermeyer M, Schlüter R, and Ney H,” “LSTM Neural Networks for Language Modeling,” in Proc. *Interspeech*. pp. 601-608, 2012.

[48] Gers F A, Schmidhuber J, and Cummins F, “Learning to forget: continual prediction with LSTM,” *Neural Computation*, vol. 12, no. 10, pp. 2451, 2000.

[49] A. Graves, “Generating sequences with recurrent neural networks,”*In Arxiv preprint arXiv*: 1308.0850, 2013.

[50] A. Graves and J. Schmidhuber, “Framewise Phoneme Classification with Bidirectional LSTM and Other Neural Network Architectures,” *Neural Networks*, vol. 18, no. 5-6, pp. 602-610, June/July 2005.

周环 于 2014 年在四川大学计算机科学与技术专业获得学士学位。现在中国科学院信息工程研究所信息安全专业攻读硕士学位。研究领域为大数据分析安全。研究兴趣包括口令安全、机器学习、Web 安全。Email: zhouhuan@iie.ac.cn



刘奇旭 于 2011 年获得中国科学院研究生院工学博士学位。现任中国科学院信息工程研究所副研究员、中国科学院大学网络空间安全学院岗位教师。研究领域为网络攻防技术、网络安全评测。研究兴趣包括: Web 安全、恶意代码分析。Email: liuqixu@iie.ac.cn

崔翔 于 2012 年在中国科学院计算技术研究所信息安全专业获得博士学位。现任广州大学网络空间先进技术研究院研究员。研究领域为网络攻防技术、网络安全评测。研究兴趣包括: 恶意代码分析、Web 安全。Email: cuixiang@iie.ac.cn

张方娇 于 2014 年在北京邮电大学计算机科学与技术专业获得硕士学位。现任中国科学院信息工程研究所助理研究员。研究领域为网络攻防技术。研究兴趣包括: 恶意代码分析。Email: zhangfangjiao@iie. ac.cn