Web安全技术

Web Security

课程大作业

刘奇旭

liuqixu@iie.ac.cn

中科院信工所 第六研究室

中国科学院大学
University of Chinese Academy of Sciences

课程成绩

- CTF之Web安全中期考核：**10%**
- CTF之Web安全期末考核：**10%**
- 大作业：**30%**
- 期末考试：**50%**

课程成绩

大作业

- **大作业：30%**
  - 大作业一个
  - 分组进行
  - 要求：认真思考，按时提交
  - 布置时间：待选课结束之后

大作业内容：方案一

口令

- 口令(Password)常用于进入：计算机、加密文件、邮箱、社交网站、网银、电子商务、即时通工具等。
- 每个人一般拥有2~6个口令，用得最多的口令包括：password, 123456, iloveyou, qwert, football等。

用户名“admin”、密码“123456”，乌克兰军方系统安全问题被曝光

Andy.i 2018-09-27 共10416人围观，发现 1 个不明物体 资讯

“123456、admin”在2017年弱密码TOP 100中，分别位列第一位和第十一位。大多数账户系统在注册时基本禁止使用这种“网红弱密码”，你很难想象这竟然会成为一个国家军方系统的用户名和密码。

9月25日，乌克兰记者 @alexdubinskyi 爆料称，乌克兰武装部队的第聂伯罗军队自动化控制系统的服务器用户名和密码分别为“admin”、“123456”。据了解，该系统主要用于协调顿巴斯地区的军事行动，也就是从2014年至今乌克兰和俄罗斯频繁交火的地区。

最先发现这个问题的是一名数据专家 Vlasyuk Dmitry，在5月22日对该系统进行网络测试的时候发现，很多服务器可以通过简易的用户名（admin）和密码（admin或者123456）访问，他及时汇报了这个安全隐患，但一段时间之后这个问题并没有得到改善。

5月25日，Vlasyuk 在邮件服务器上发现了类似的情况，基本上不需要技术很高深的黑客就能够轻松访问交换机、路由器、服务器、打印机和扫描仪等设备，能够分析出武装部队大量的机密信息甚至掌握整个夏天乌克兰军队在顿巴斯地区的一切计划。

口令泄漏事件

CSDN
全球最大中文IT社区

- **2011-12-21：有网友爆料称，今天有黑客在网上公开了知名网站CSDN的用户数据库，这是一次严重的暴库泄密事件，涉及到的账户总量高达600万。**

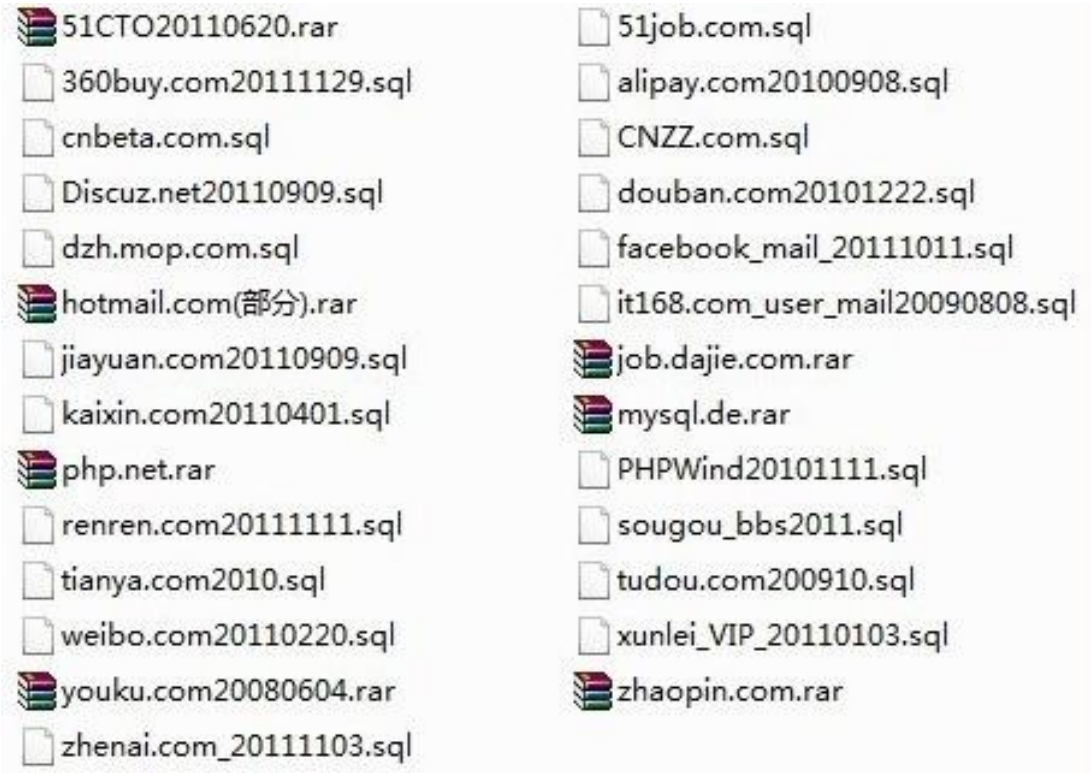
中国科学院大学
University of Chinese Academy of Sciences

口令泄漏事件——爆发

- 21日16时左右，网友“潇洒小姐燕子”在微博上列出一长串名单，除了CSDN，有同样问题的大网站还有CNBETA、CNZZ、ENET硅谷动力、百合网、珍爱网、开心网、YY、酷6等，并上传了一个类似数据库的东西作为证据。
- 截至22日17时，被点名的网站均没有对此回应

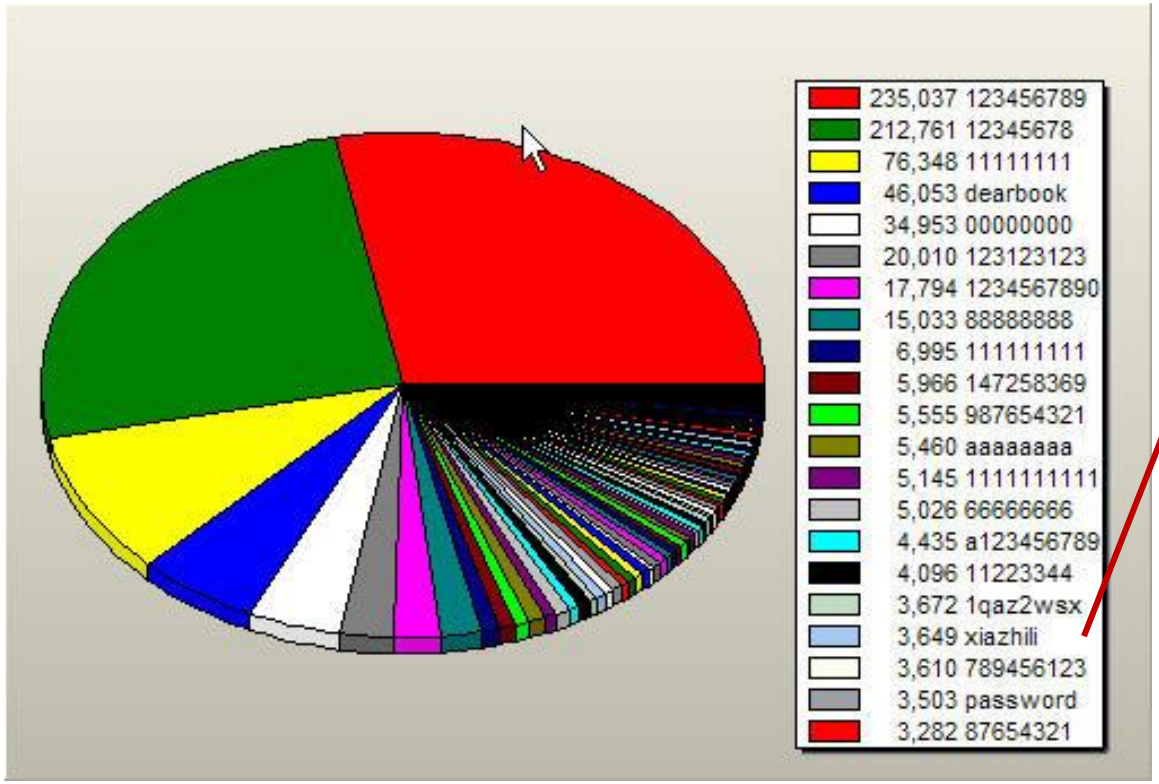
口令泄漏事件——后果


打开
包含到库中
共享
新建文件夹
名称
修改
7k7k-2000w
178-1000w
3000W_163
csdn-600w
duowan-800w
嘟嘟牛-1600w
人人网 -500w
3000W_16328.rar
猫扑1000W_85695.rar
的位置
CSDN-中文IT社区-600万.rar
104.85 MB
多玩网_800W.rar
216.91 MB
人人网500W_16610.rar
49.56 MB
猫1000W_8228.rar
91.94 MB
7k7k2000万_2047.rar
194.21 MB


51CTO20110620.rar
360buy.com20111129.sql
cnbeta.com.sql
Discuz.net20110909.sql
dzh.mop.com.sql
hotmail.com(部分).rar
jiayuan.com20110909.sql
kaixin.com20110401.sql
php.net.rar
renren.com20111111.sql
tianya.com2010.sql
weibo.com20110220.sql
youku.com20080604.rar
zhenai.com_20111103.sql
51job.com.sql
alipay.com20100908.sql
CNZZ.com.sql
douban.com20101222.sql
facebook_mail_20111011.sql
it168.com_user_mail20090808.sql
job.dajie.com.rar
mysql.de.rar
PHPWind20101111.sql
sougou_bbs2011.sql
tudou.com200910.sql
xunlei_VIP_20110103.sql
zhaopin.com.rar

口令背后那点事儿

——CSDN最常用口令



xiazhili

- xiazhili 是csdn下载频道09年上传比较多的一MM会员，众多程序员yy的对象，故xiazhili作为密码不足为奇。

中国科学院大学
University of Chinese Academy of Sciences

CSDN——谁是你的最爱

- CSDN杯我最喜爱的CSDN密码活动，统计了一下包含ilove***的密码，其中被爱得死去活来的前20位如下：

排名	ilove***	口令数量
1	you	3567
2	you1314	110
3	U	92
4	csdn	68
5	you123	57
6	china	49
7	you520	43
8	thisgame	41
9	java	31
10	chu	20

排名	ilove***	口令数量
11	123	30
12	2hcx	29
13	you1	26
14	myself	22
15	you521	22
16	r	19
17	jay	19
18	qsr	18
19	520	18
20	1314	18

CSDN——爱的就是你

- 排在最前的国家是：**China**
- 排在最前的网站是：**csdn**
- 排在最前的编程语言是：**Java**
- 排在最前的操作系统是：**Linux**
- 排在最前的电脑品牌是：**apple**
- 排在最前的明星是：**周杰伦**
- 排在最前的动物分别是：
  - 1. 猪
  - 2. 猫
  - 3. 猪头
  - 4. 狗

- 排在最前的mm名字是
  1. yan（燕）
  2. mei（梅）
  3. jing（静）
  4. ling（玲）
  5. ping（萍）
  6. dan（丹）
  7. fang（芳）
  8. wei（薇）
  9. juan（娟）
  10. nana（娜娜）

CSDN——爱的就是你

学术状态帝
@xueshudi

暗恋了她好几年，一直不敢表白。后来，他下载到一份CSDN泄露的用户名密码名单，习惯性的查找她的邮箱，发现她使用的是ilove加自己名字的拼音作为密码，正感动得无以复加时电话响起，只听她在电话那头颤抖着说：傻瓜，我看到了你的密码。——程序猿伤不起啊。。故事好感人啊。。

翻译自中文

2017/9/27 上午9:43

CSDN——EDU.CN

排名	域名	数量	归属
1	mail.ustc.edu.cn	2035	中国科学技术大学
2	sjtu.edu.cn	1874	上海交通大学
3	bjtu.edu.cn	1322	北京交通大学
4	fudan.edu.cn	981	复旦大学
5	stu.xjtu.edu.cn	929	西安交通大学
6	zju.edu.cn	872	浙江大学
7	mails.tsinghua.edu.cn	718	清华大学
8	bit.edu.cn	691	北京理工大学
9	mail.nankai.edu.cn	640	南开大学
10	stu.edu.cn	554	汕头大学

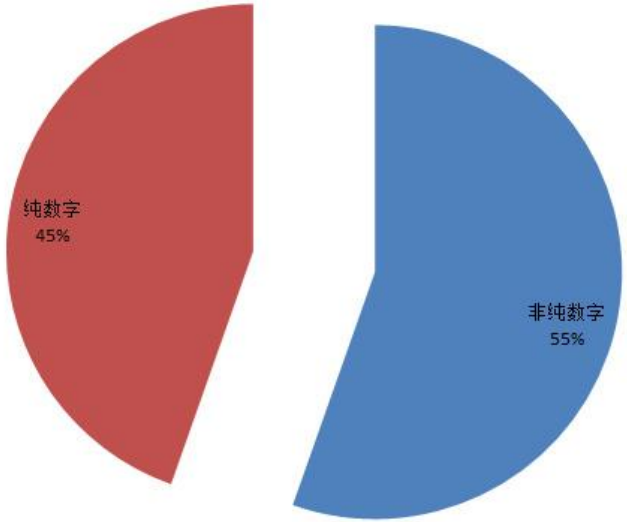
CSDN——口令生成的艺术

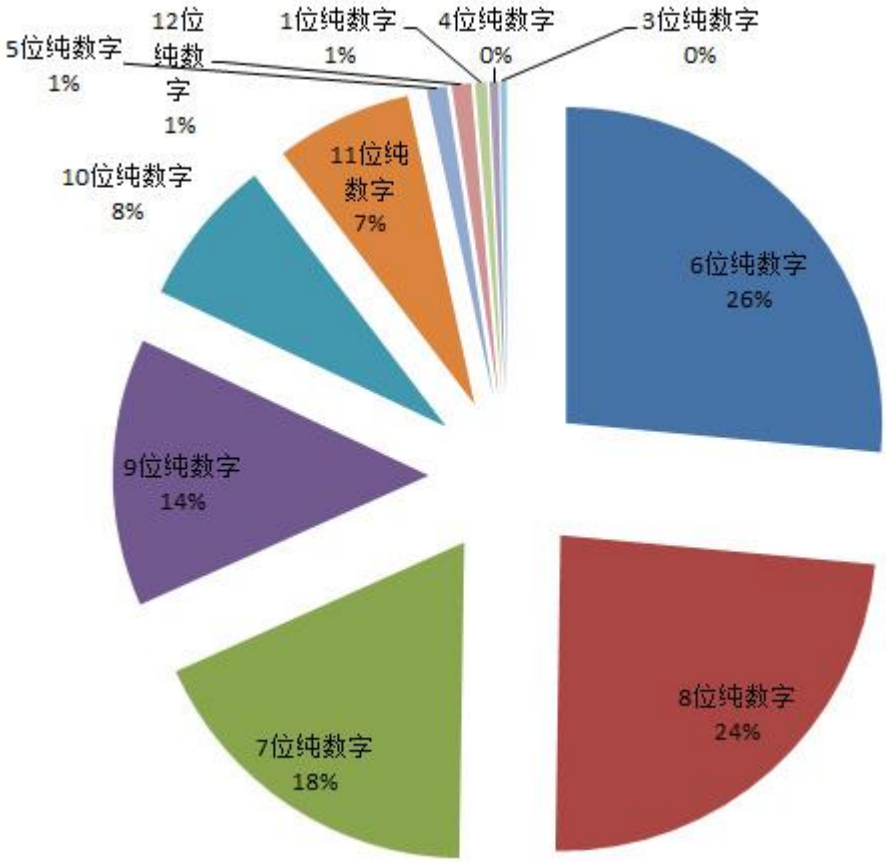
- CSDN的600万用户数据被泄露后，有人发现其中几个最牛的密码：

鱼和熊掌不可兼得	
hold?fish:palm	
hanshansi.location()!∈[gusucity]	FLZX3000cY4yhx9day
姑苏城外寒山寺	飞流直下三千尺，疑似银河下九天

全部泄露口令——纯数字的比例

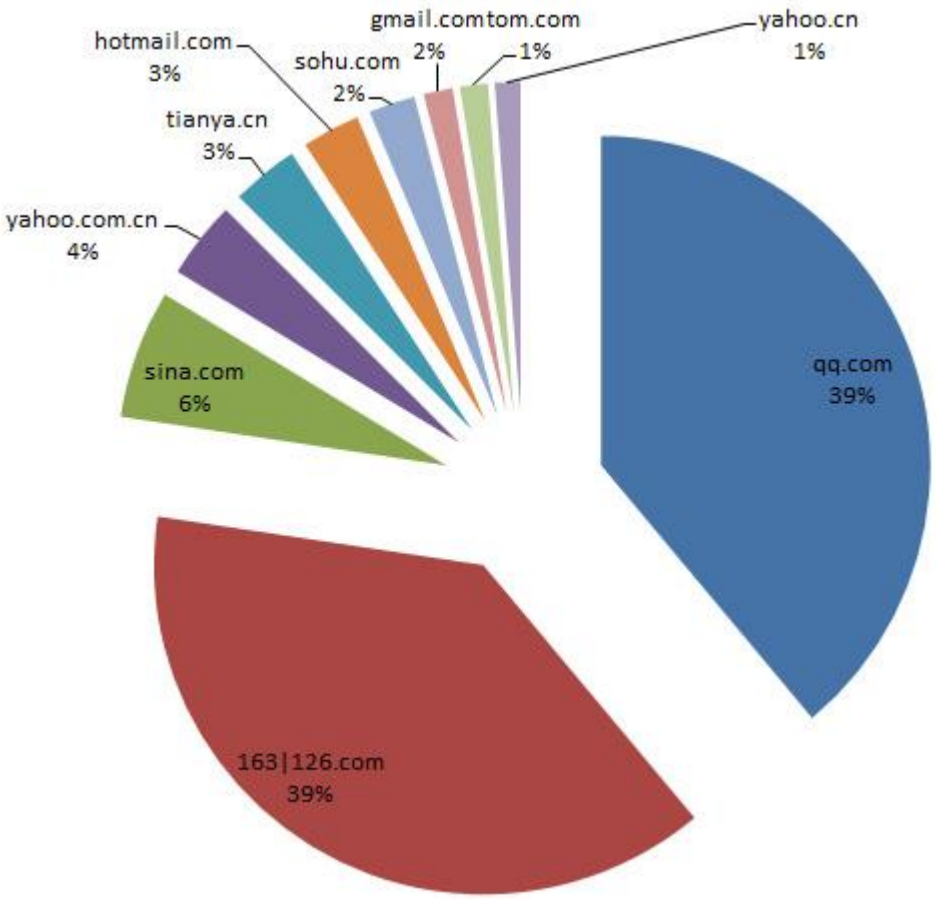
- 45%之巨（大约1700万）的被统计用户选择了纯数字作为他们的密码，这反应出国内大多数网民安全意识还相当淡薄





全部泄露口令——纯数字的比例

- 网易和腾讯几乎瓜分了80%的市场份额，在本次统计中两者差距在10万以内



中国科学院大学
University of Chinese Academy of Sciences

规律性?

口 为了便于记忆，口令结构和设置方法一般都具有规律性

- 口令结构规律
- 口令设置方法规律

- 例如：password123! 规律$L_8D_3S_1$
- MySpace口令统计规律
  - L_6D_1是最常见的口令结构，占9.98%，例如loveme8
  - 1是使用最多的数字，占所有数字的27.47%
  - !是使用最多的特殊字符，占38.46%

口令安全研究

用户脆弱口令行为

- 用户倾向性构造模式选择
- 口令重用
- 基于个人信息构造口令

口令猜解攻击算法

“奇思妙想” → 概率模型科学化算法

- PCFG: 概率上下文无关方法 (probabilistic context-free grammars)
- Markov-Chain: 马尔科夫链
- Natural Language Processing:自然语言处理技术

口令猜解攻击

漫步攻击

漫步攻击（trawling attacking）是指攻击者不关心具体的攻击对象是谁，其唯一的目标是在允许的猜测次数下，猜测出越多的口令越好。

漫步攻击算法：

- 启发式算法
- PCFG
- Markov
- NLP

参考文献

计算机研究与发展
Journal of Computer Research and Development

DOI:10.7544/issn1000-1239.2016.20160483
53(10):2173-2188,2016

口令安全研究进展

王 平[1,3] 汪 定[1] 黄欣沂[2]

[1](北京大学信息科学技术学院 北京 100871)

[2](福建师范大学数学与计算机科学学院 福州 350117)

[3](北京大学软件与微电子学院 北京 102600)

(wangdingg@pku.edu.cn)

Advances in Password Security

Wang Ping[1,3], Wang Ding[1], and Huang Xinyi[2]

[1](*School of Electronics Engineering and Computer Science, Peking University, Beijing* 100871)

[2](*School of Mathematics and Computer Science, Fujian Normal University, Fuzhou* 350117)

[3](*School of Software and Microelectronics, Peking University, Beijing* 102600)

口令猜解攻击

定向攻击

定向攻击（targeted attacking）中攻击者会利用与攻击对象相关的个人信息（personal information,PI），以增强猜测的争对性。

个人信息有很多种，比如人口学相关信息（姓名、生日、职业等），用户在该网站的过期口令（旧口令），用户在其他网站泄露的口令。

当前定向口令猜测研究尚在起步阶段。

定向攻击算法:

Targeted-Markov

Personal-PCFG

其核心是训练之前先将PI分类（用户名 A、邮箱 E、姓名N、生日B、手机号P、身份证G等），并将其看作是L、D、S一样的组件，猜测生成阶段仿照传统Markov和PCFG方法即可。

网络与系统安全顶级会议

S&P (Oakland)	IEEE Symposium on Security and Privacy
CCS	ACM Conference on Computer and Communications Security
Security	Usenix Security Symposium
NDSS	ISOC Network and Distributed System Security Symposium

2014	23rd USENIX Security Symposium	San Diego, CA

Safer Sign-Ons

Harbor DEF

Session Chair: Tadayoshi Kohno, *Microsoft Research and University of Washington*

Password Managers: Attacks and Defenses

David Silver, Suman Jana, and Dan Boneh, *Stanford University;* Eric Chen and Collin Jackson, *Carnegie Mellon University*

The Emperor's New Password Manager: Security Analysis of Web-based Password Managers

Zhiwei Li, Warren He, Devdatta Akhawe, and Dawn Song, *University of California, Berkeley*

SpanDex: Secure Password Tracking for Android

Landon P. Cox , Peter Gilbert, Geoffrey Lawler, Valentin Pistol, and Ali Razeen, Bi Wu, and Sai Cheemalapati, *Duke University*

SSOScan: Automated Testing of Web Applications for Single Sign-On Vulnerabilities

Yuchen Zhou and David Evans, *University of Virginia*

Passwords

Harbor DEF

Session Chair: David Wagner, *University of California, Berkeley*

A Large-Scale Empirical Analysis of Chinese Web Passwords

Zhigong Li and Weili Han, *Fudan University;* Wenyuan Xu, *Zhejiang University*

Password Portfolios and the Finite-Effort User: Sustainably Managing Large Numbers of Accounts

Dinei Florêncio and Cormac Herley, *Microsoft Research;* Paul C. van Oorschot, *Carleton University*

Telepathwords: Preventing Weak Passwords by Reading Users' Minds

Saranga Komanduri, Richard Shay, and Lorrie Faith Cranor, *Carnegie Mellon University;* Cormac Herley and Stuart Schechter, *Microsoft Research*

Towards Reliable Storage of 56-bit Secrets in Human Memory

Joseph Bonneau, *Princeton University;* Stuart Schechter, *Microsoft Research*

2015	24th USENIX Security Symposium	Washinton, D.C.

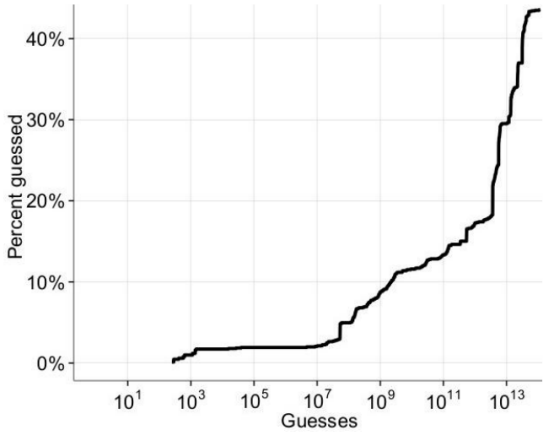
usenix
THE ADVANCED COMPUTING SYSTEMS ASSOCIATION

Measuring Real-World Accuracies and Biases in Modeling Password Guessability

Blase Ur, Sean M. Segreti, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor, Saranga Komanduri, and Darya Kurilova, *Carnegie Mellon University;* Michelle L. Mazurek, *University of Maryland;* William Melicher and Richard Shay, *Carnegie Mellon University*

https://www.usenix.org/conference/usenixsecurity15/technical-sessions/presentation/ur

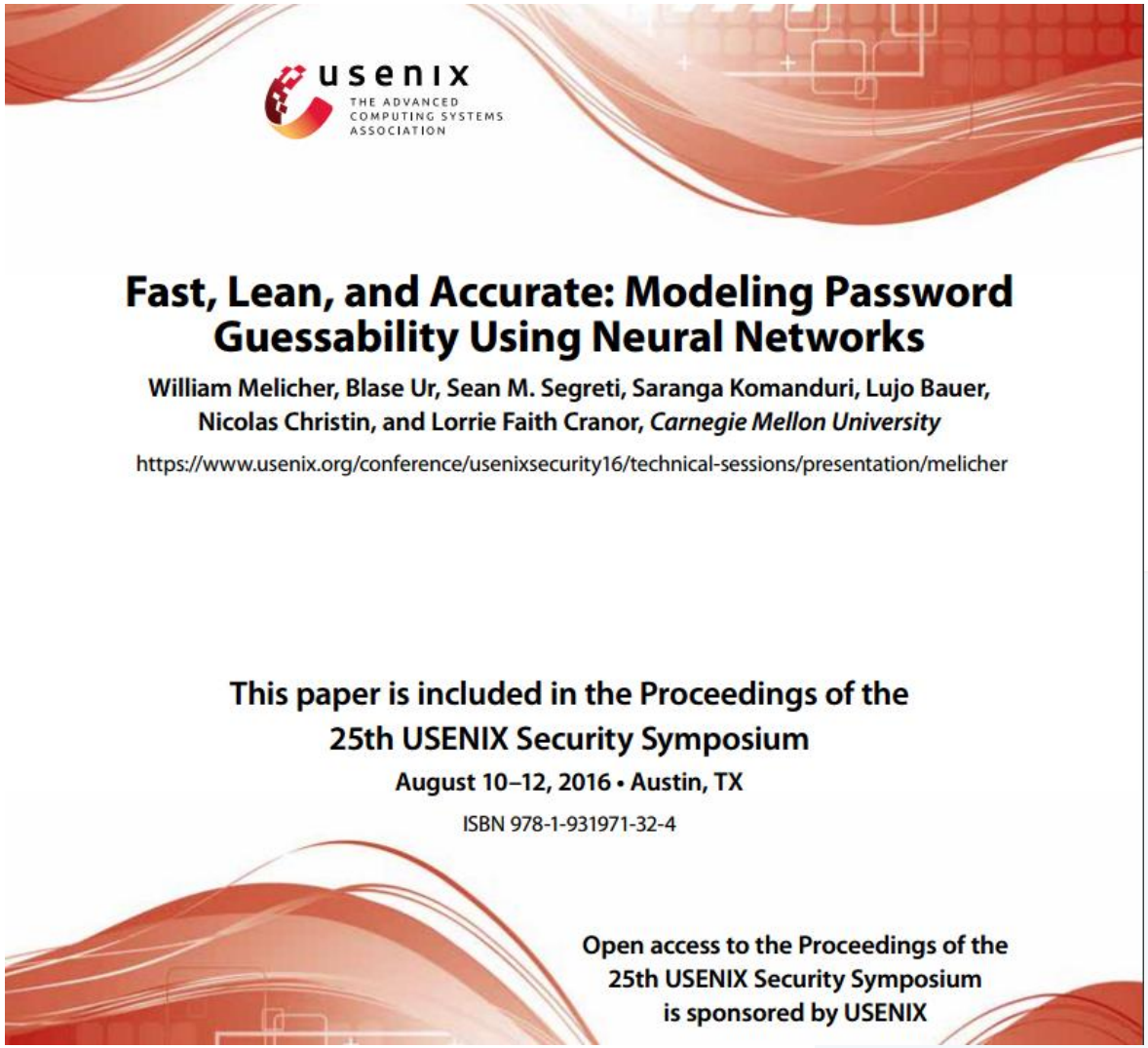
Guessability Plots

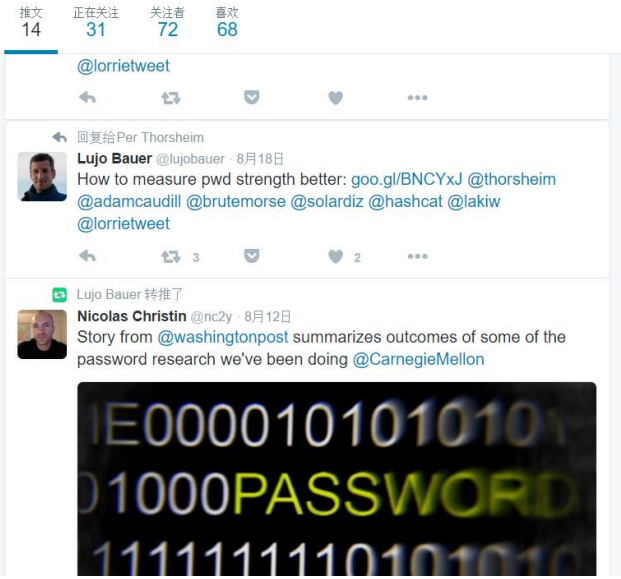


This paper is included in the Proceedings of the
24th USENIX Security Symposium
August 12–14, 2015 • Washington, D.C.
ISBN 978-1-931971-232

Open access to the Proceedings of
the 24th USENIX Security Symposium
is sponsored by USENIX

2016	25th USENIX Security Symposium	AUSTIN, TX





2018	The 25th ACM Conference on Computer and Communications Security (CCS 2018)	Toronto, Canada

On the Accuracy of Password Strength Meters

Maximilian Golla
Ruhr University Bochum
Bochum, Germany
maximilian.golla@rub.de

Markus Dürmuth
Ruhr University Bochum
Bochum, Germany
markus.duermuth@rub.de

A METER COMPARISON

In the following, we list the full results of our data collection. We separated the five categories *Academic Proposals*, *Password Managers*, *Operating Systems*, *Websites*, and *Previous Work* into two tables. A colorful version that allows easier comparison can be found online [29].

A.1 Academic Proposals, Password Managers, and Operating Systems

Table 5: We computed the weighted Spearman correlation as the best similarity score (cf. Section 5). The table lists the online use case on the left, the offline use case on the right. We highlighted if and on how many bins a meter quantized its output. Additionally, we list whether a meter runs on client- or server-side and how the meter visualizes the strength to the user.

ID	Meter	Type	Quant.	Visu.	Online Attacker			Offline Attacker		
					RockYou	LinkedIn	000Webhost	RockYou	LinkedIn	000Webhost
					Academic Proposals					
1A	**Comprehensive8** [61]	C	-	-	-0.652	-0.589	0.251	-0.476	-0.616	0.441
1B	**Comprehensive8** [61]	C	Q5	Text	-0.331	-0.084	0.409	-0.128	-0.123	0.421
2	**Eleven** [22]	C	-	-	0.670	0.912	0.492	0.755	0.951	0.733
3	**LPSE** [32]	C	Q3	-	0.584	0.669	0.508	0.544	0.718	0.693
4A	**Markov (OMEN)** [13]	S	-	-	0.721	0.697	0.410	0.701	0.669	0.660
4B	**Markov (Single)** [27]	S	-	-	0.718	0.998	0.817	0.828	0.991	0.872
4C	**Markov (Multi)** [27]	S	-	-	0.721	0.998	0.902	0.997	0.995	0.777
5A	**NIST** [11]	C	-	-	0.670	0.912	0.492	0.755	0.951	0.733
5B	**NIST (w. Dict.)** [11]	C	-	-	0.669	0.910	0.472	0.756	0.953	0.816
6	**PCFG (fuzzyPSM)** [65]	S	-	-	1.000	0.994	0.963	0.998	0.999	0.899
7A	**RNN Generic** [46]	C	-	-	0.632	0.542	0.427	0.535	0.520	0.800
7B	**RNN Generic (Web)** [59]	C	-	-	0.473	0.649	0.421	0.449	0.688	0.777
7C	**RNN Target** [46]	C	-	-	0.951	0.913	0.965	0.896	0.860	0.885
7D	**RNN Target (w. Bloom)** [46]	C	-	-	0.951	0.913	0.965	0.896	0.860	0.882
8A	**zxcvbn (Guess Number)** [71]	C	-	-	0.989	0.990	0.554	0.989	0.999	0.868
8B	**zxcvbn (Score)** [71]	C	Q5	-	0.341	0.490	0.359	0.373	0.567	0.817

大学 of Sciences

Password Leakage

English

rockyou

YAHOO!

Chinese

CSDN
全球最大中文IT社区

天涯社区
www.tianya.cn

嘟嘟牛
WWW.DODONEW.COM

7k7k

178.COM

Over 100 million plaintext passwords

作业要求

分析目标

国内

CSDN
全球最大中文IT社区

600W

国外

YAHOO!

73W

快讯 | 雅虎承认其30亿用户信息全部被黑

Akane 2017-10-05 共14246人围观 资讯

近日，已被Verizon电信收购的雅虎公司宣布2013年8月发生的大规模数据泄露事件，影响范围包括所有雅虎用户，这意味着全球30亿雅虎账户无一幸免。据悉，雅虎最初只披露了10亿用户账号被泄露，后续也有陆续增加，但昨天的公告表明，如果你有一个雅虎账号，那么很不幸，你也被曝光了。

去年12月15日，雅虎承认，其系统曾在2013年遭到黑客攻击，约10亿账号的**用户姓名、生日、邮箱地址、密码、电话、安全问题和答案**全被泄露。除2013年的重大泄露事件以外，雅虎2014年也有至少5亿用户资料落入黑客之手。

作业要求

分组：每组1-7人

1、基础分析（选择下列内容中的三种进行分析）：

① 密码构成元素分析（数字、字符、字母等）和结构分析，得到密码中这些基本元素常用的组合方法；

② 键盘密码的模式分析，键盘密码就是基于键位变化的一类密码，比如asdfgh；

③ 日期密码及其格式分析，难点在于识别日期密码，区分不同的日期格式，日期与其他字符混排的组合方式统计

④ 拼音的使用统计，Top10，大小写等，难点是如何识别

⑤ 英文单词的使用统计，Top10，大小写等，难点是如何识别

⑥ 其他，可以自己想

⑦ 其他，可以自己想

⑧ 其他，可以自己想

2、基于分析结果，实现一种口令猜测攻击算法，并生成口令字典。（推荐编程语言：Python）

大作业内容：方案二

分组：每组1-7人

自　选

基于口令相关顶级学术论文

大作业内容：方案三

人员组成：每组1-7人

网络空间安全领域更值得交流分享的内容

（选题需征得老师同意）

大作业时间节点

月份 month	九月(Sep)				十月(Oct)				十一月(Nov)				
周次 week	1	2	3	4	5	6	7	8	9	10	11	12	13
星期一（Mon）	3	10	17	24 中秋节	1 国庆节	8	15	22	29	5	12	19	26
星期二（Tue）	4	11	18	25	2	9	16	23	30	6	13	20	27
星期三（Wed）	5	12	19	26	3	10	17	24	31	7	14	21	28
星期四（Thu）	6	13	20	27	4 中秋节	11	18	25	1	8	15	22	29
星期五（Fri）	7	14	21	28	5	12	19	26	2	9	16	23	30
星期六（Sat）	8	15	22	29	6	13	20	27	3	10	17	24	1
星期日（Sun）	9	16	23	30	7	14	21	28	4	11	18	25	2

作业布置　　作业提交　　课堂交流(暂定)

作业提交

- **确定分组、各组自行指定组长**
  - 2018年10月10日之前，组长联系助教杨粟，将组员名单发给助教yangs@nipc.org.cn，分组名单包括姓名、学号。
- **提交时间：2018年11月10日23：00**
- **提交内容：**
  - 【必须】分组名单-指定组长
  - 【必须】课堂交流PPT
  - 【必须】相关程序源代码、程序使用说明
  - 【可选】附属材料（相关视频、参考资料等）
- **格式要求**
  - ***各组组长***以压缩包的形式上传到课程网站，组员无需上传。若压缩包太大，可以单独联系老师，通过其他方式提交大作业。建议压缩包命令规则：学号_姓名.rar

作业提交

课程网站

中国科学院大学
University of Chinese Academy of Sciences

[2018秋]Web Security

扫一扫二维码，加入群聊。

谢谢大家

刘奇旭

liuqixu@iie.ac.cn

中科院信工所 第六研究室

中国科学院大学
University of Chinese Academy of Sciences