北京大学
PEKING UNIVERSITY

Honeywords 改进

杨雨月 贾云龙 兰阳 楚选耕

目录

1 相关文献简介

Honeywords和Threshold Schemes的相关文献

2 本项目的改进技术

本项目的主要改进点

3 实现方案

本项目项目结构介绍

4 演示

Demo程序演示

相关文献简介

Honeywords与Threshold Schemes

相关文献简介

Honeywords与Threshold Schemes

Honeywords: making password-cracking detectable

Authors: Juels, Ari, Rivest, Ronald L

Abstract: We propose a simple method for improving the security of hashed passwords: the maintenance of additional ‘honeywords’ (false passwords) associated with each user's account. An adversary who steals a file of hashed passwords and inverts the hash function cannot tell if he has found the password or a honeyword. The attempted use of a honeyword for login sets off an alarm. An auxiliary server (the ‘honeychecker’) can distinguish the user password from honeywords for the login routine, and will set off an alarm if a honeyword is submitted.

Key words: authentication chaffing honeywords login password cracking password hashes passwords

Honeywords: making password-cracking detectable

一种检测泄露攻击的方法

Honeywords是一种向密码中混入**伪密码**的方法。用于检测**盗取服务器密码文件**而试图登陆的攻击。

系统通过Honeychecker来检测登陆信息。如果是正确密码则登入，如果不是，检测是否是 Honeywords。如果该系统检测到是 Honeywords 非法登陆，即报警通知管理员采取措施。

生成策略：避免简单的错误如少量或单个拼写错误即使正确密码转变为Honeywords。如果错误位点太少，正常用户就有概率触发Honeywords警报。

抵御散列函数攻击：很多用户喜欢使用基于语义的密码。对于此类密码，尽可能使Honeywords也符合自然语言规律。否则不需要散列函数也可以轻易辨别出真正的密码。

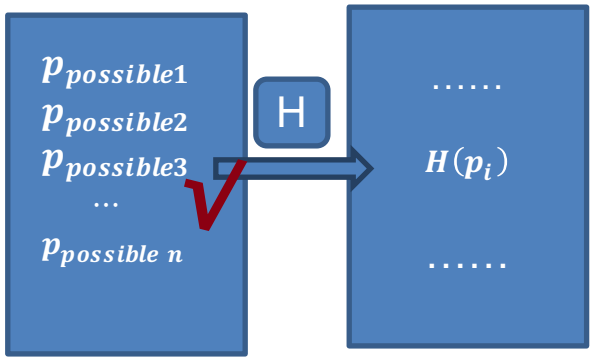
反向攻击模型

明文 u_i

哈希 $H(p_i)$

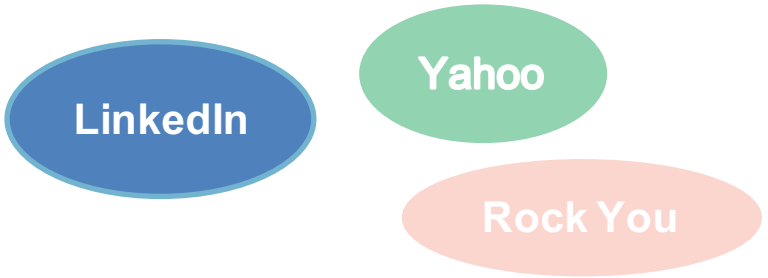
Adversary

$H(p_i) \rightarrow p_i$



暴力攻击

反向攻击模型



暴力攻击

时间复杂度高，因为攻击者试图使用各种可能

2008年 John、Ripper

一种能够显著降低反向攻击时间复杂度的公开密码破解算法

2009年 Weir等人

基于概率上下文无关语法的概念，能够破解28%-129%的口令

最近 Ma等人

使用马尔可夫链模型进行密码破解

应对方案

1）将用户的密码转换为更难反转的哈希值

增加了登录时间，并且不会使成功的密码破解可被检测

2）由管理员设置几个假登录帐户，成功反转任何此类帐户哈希值的对手，都会被系统检测到

经过仔细分析，对手可以区分真实用户名和系统生成的用户名

3）Honeywords

系统维护一个密码列表，其中包含真实用户的密码以及一些系统生成的密码，称为honeywords。系统通过使用诸如take-a-tail、modelling syntax等生成算法来生成honeywords。一旦密码文件被泄露并且对手从Wi的密码列表中输入任何honeywords，系统就识别攻击,采取必要的行动。

相关文献简介

Honeywords与Threshold Schemes

How to share a secret

Authors: Adi Shamir

Abstract: In this paper we show how to divide data D into n pieces in such a way that D is easily reconstructable from any k pieces, but even complete knowledge of k - 1 pieces reveals absolutely no information about D. This technique enables the construction of robust key management schemes for cryptographic systems that can function securely and reliably even when misfortunes destroy half the pieces and security breaches expose all but one of the remaining pieces.

Key words: cryptography, key management, interpolation

How to share a secret

一种抵御泄露攻击的方法

Shamir's Threshold Schemes是一种**分布式存储密码**的方法。用于抵御**盗取服务器密码文件**的攻击行为。

该方法由Adi Shamir最早提出，这种 (k,n) 加密方法将秘密 S 分为 n 个子秘密，任意 k 个子秘密都可以恢复出 S，而任意 $k-1$ 个子秘密都无法恢复出 S。

生成策略：经典的Shamir secret sharing算法通过多项式方法构建。取任意随机数$a_1,\dots,a_{k-1}$，令$a_0 = S$，构建多项式

$$f(x) = a_0 + a_1x_1 + \cdots + a_{k-1}x_{k-1}$$

存储$(x_1,f(x_1)),\dots,(x_n,f(x_n))$到 n 个服务器上。

解密策略：这种情况下，任意 k 个值对可以求解出多项式中$a_0,\dots,a_{k-1}$的值。将 $x=0$ 代入即可得到原秘密 S。而获知任何小于 k 个值对都无法求解多项式的确切值。

本项目的改进技术

主要改进点

脆弱性分析（一）

存储开销

系统需要为每个用户帐户存储k-1多个密码，很大程度上增加了存储成本。

关联危险

如果用户名和密码之间存在关系，那么用户的原始密码容易识别。这种情况，蜜词不能掩盖原始密码。

可区分的已知密码模式

如果用户使用与一些已知对象/事实相关的密码，则攻击者可以容易地识别原始密码。

拒绝服务攻击

如果对手在知道用户原始密码时可以猜出蜜字，那么对手可以故意提交蜜字。如果系统检测到来自太多帐户的蜜词提交，那么系统可能会阻塞整个Web服务器。

多系统漏洞

如果用户在多个不同系统中使用相同的密码，并且对手获得对两个系统的访问，则可能出现多系统漏洞。

类型安全问题

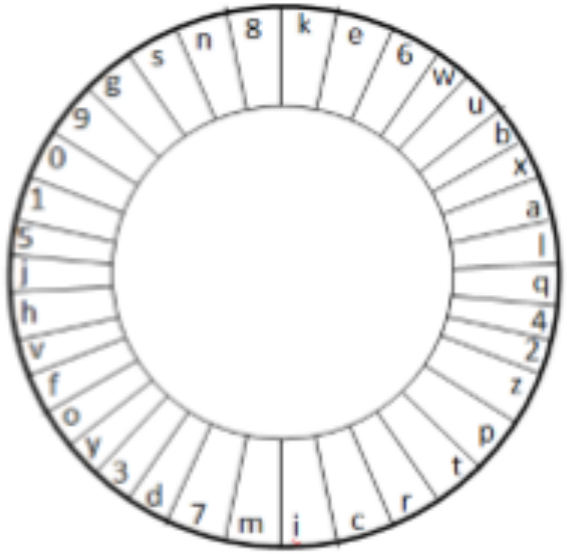
合法用户可能会意外地提交一个蜜字。

PDP协议

Enter Username :	Alice
Enter Password Choice :	******
Choose a random string to complete your password	
Enter Revised Password :	**********

用户需要提供 ：用户名、口令、随机字符串RS
RS的默认长度设置为3。

优点：
1）RS是用户自己选择的；
2) RS的字符串长度较小
（考虑为3以避免像出生日期这样的特殊模式）；
3) 用户可以为不同的登录帐户使用相同的RS。



创建一个循环列表hcl，它按随机顺序保存字母表和数字。将HCl的默认值设为36。这个hcl安全地分布到m个不同的系统，参与使用PDP协议创建蜜语。hcl保存在密码文件F中。

PDP协议

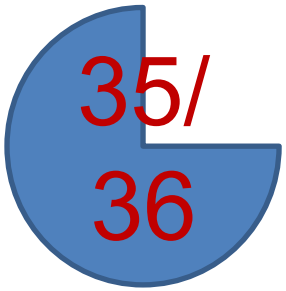
配对距离：两个元素e1和e2之间的配对距离，表示为Pr(e1，e2)是hcl中从元素E1到元素E2沿顺时针方向穿过的元素数量。

距离链：距离链是RS的每两个连续元素之间的n-1对距离的集合（由“-”分隔），长度为n。

距离链的唯一性：给定一个hcl和一个特定的距离链RS，如果RS的第一个元素是已知的，则可以唯一地导出。

选择RS的必要性：PDP的强度取决于字符串RS的随机性。

保存honeychecker
在现有方法中，通常honeychecker维护用户名和原始密码的索引。在所提出的方法中，除了用户名之外，honeychecker还保持了由用户选择的RS的第一个元素。

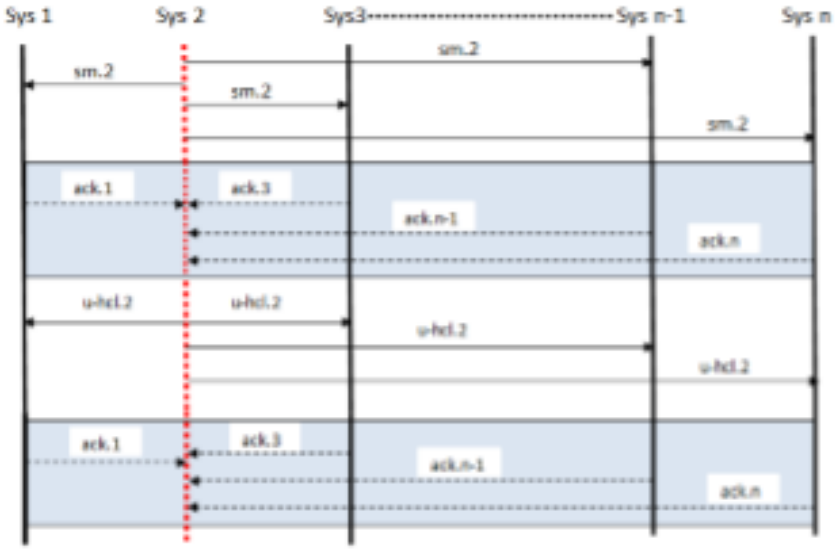


登录凭证正确

系统从提交的RS导出距离链与存储的距离链匹配

用户提交的RS的第一个元素与honeychecker中存储的元素匹配

PDP协议



Honeyword method	Flatness	DoS Resiliency	Security against MSV	System interference	Typo safety	Stress on memorability	Storage overhead
CTD	$1/k$ if U $\approx$ G	low	low	no	low	low	k-1
modelling -syntax	$1/k$ if U $\approx$ G	high	low	no	high	low	k-1
take-a- tail	$1/k$ (unconditionally)	low	high	high	high	high	k-1
PDP	$1/k$ ⊛	high	high	low	high	low	1

本项目的改进技术

主要改进点

01

更好的安全性

基于门限系统分布式存储密码使单个密码服务器被攻破无法还原出任何密码，从而使整个密码系统有更好的安全性。

02

更好的可靠性

基于门限的分布式系统有更好的可靠性。即使部分服务器损坏，只要剩余服务器高于门限数目，系统仍可以运行。

03

更好的可用性

更好的可靠性带来更高的可用性，对服务器损坏更好的抗性使整个系统宕机的可能性更小。

04

更好的吞吐量

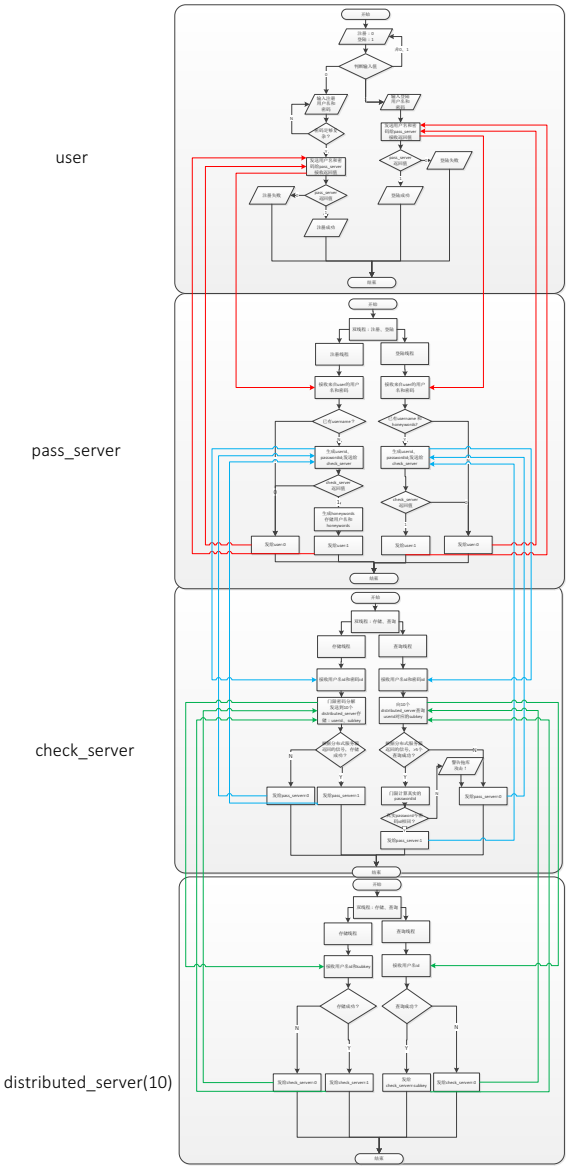
分布式系统通过负载均衡，可以使不同的请求访问不同组合的阈值数目服务器，从而极大提升整个系统的吞吐量。

实现方案

项目架构

实现方案

项目架构



演示

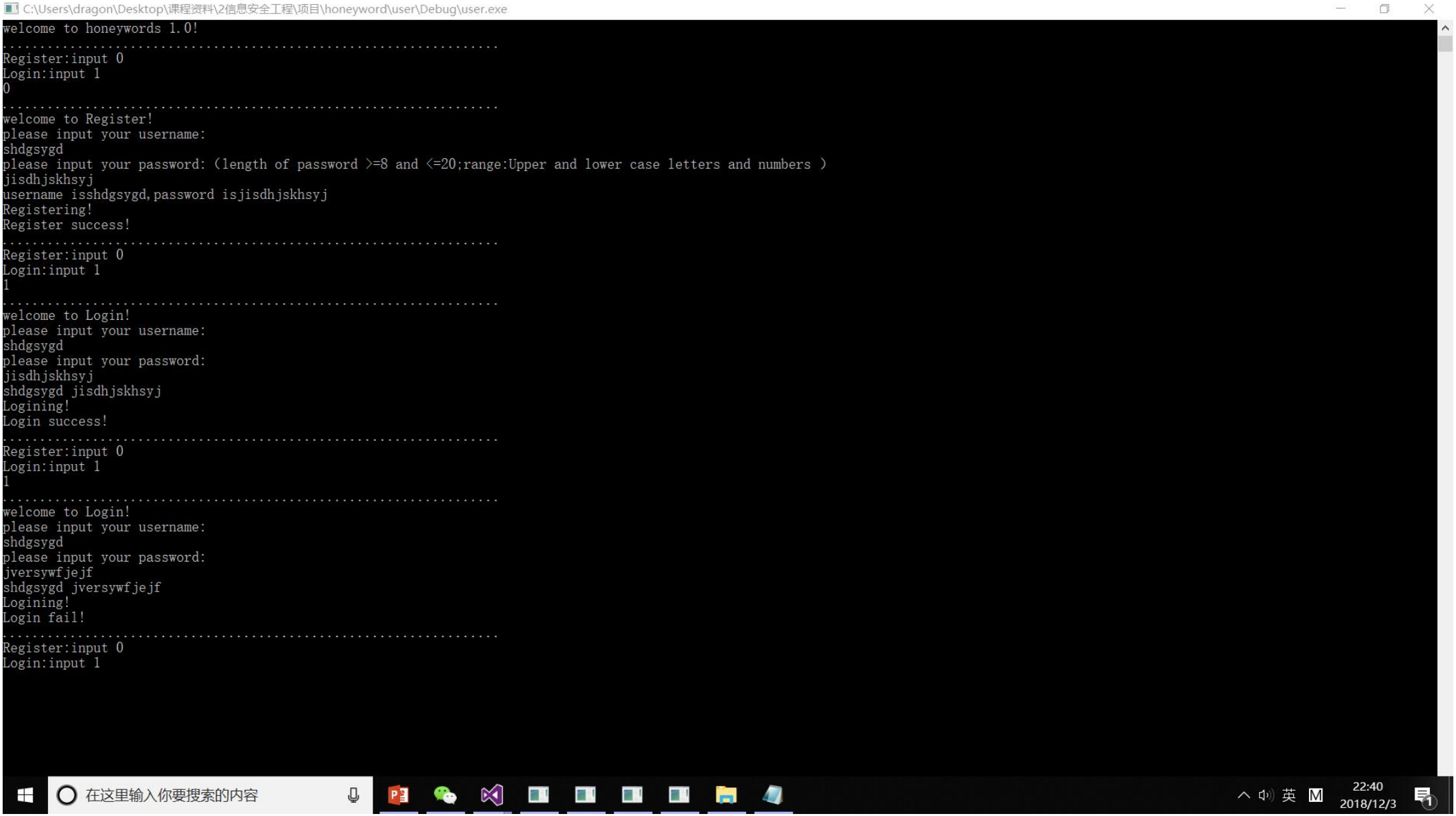
Demo程序演示

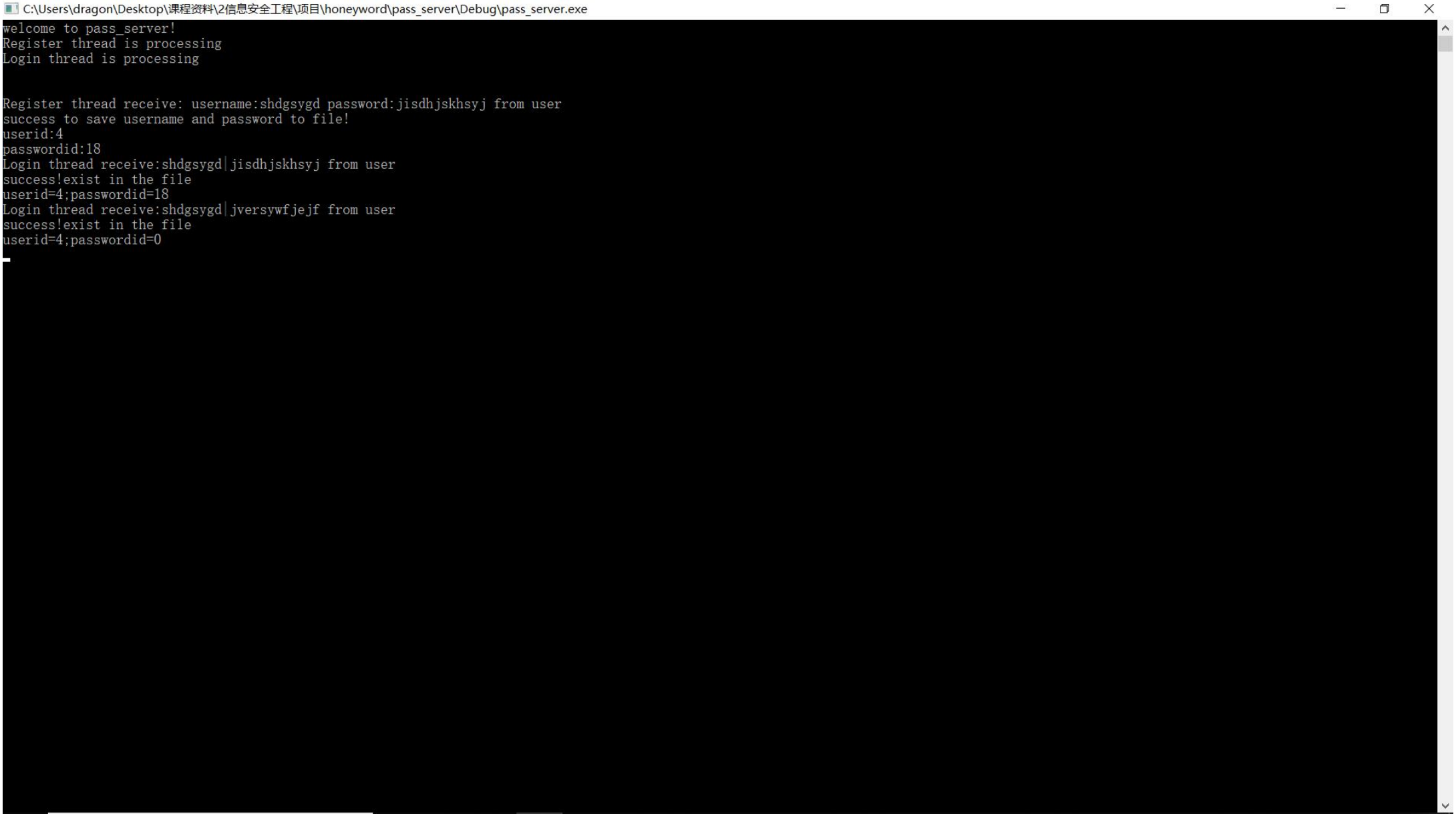
演示

程序及代码演示


Thank you

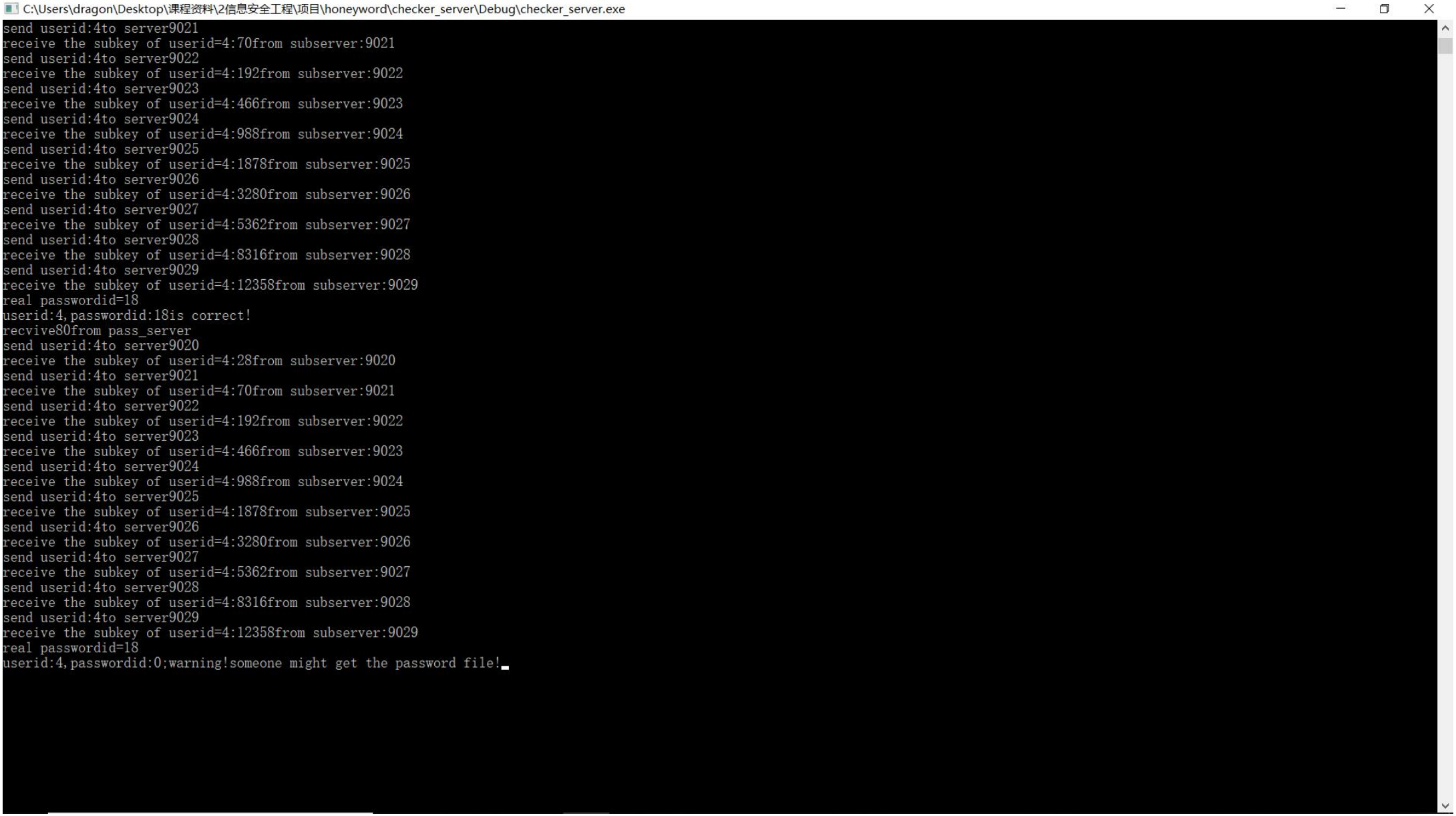
附：部分运行结果截图


C:\Users\dragon\Desktop\课程资料\2信息安全工程\项目\honeyword\user\Debug\user.exe
welcome to honeywords 1.0!
.....
Register:input 0
Login:input 1
0
.....
welcome to Register!
please input your username:
shdgsygd
please input your password: (length of password >=8 and <=20;range:Upper and lower case letters and numbers)
jisdhjskhsyj
username isshdgsygd,password isjisdhjskhsyj
Registering!
Register success!
.....
Register:input 0
Login:input 1
1
.....
welcome to Login!
please input your username:
shdgsygd
please input your password:
jisdhjskhsyj
shdgsygd jisdhjskhsyj
Logining!
Login success!
.....
Register:input 0
Login:input 1
1
.....
welcome to Login!
please input your username:
shdgsygd
please input your password:
jversywfjejf
shdgsygd jversywfjejf
Logining!
Login fail!
.....
Register:input 0
Login:input 1
在这里输入你要搜索的内容
英
22:40
2018/12/3


C:\Users\dragon\Desktop\课程资料\2信息安全工程\项目\honeyword\pass_server\Debug\pass_server.exe
welcome to pass_server!
Register thread is processing
Login thread is processing
Register thread receive: username:shdgsygd password:jisdhjskhsyj from user
success to save username and password to file!
userid:4
passwordid:18
Login thread receive:shdgsygd|jisdhjskhsyj from user
success!exist in the file
userid=4;passwordid=18
Login thread receive:shdgsygd|jversywfjejf from user
success!exist in the file
userid=4;passwordid=0

C:\Users\dragon\Desktop\课程资料\2信息安全工程\项目\honeyword\checker_server\Debug\checker_server.exe

```
welcome to check_server!
Register thread is processing!
check thread is processing!
recvive98from pass_server
28
70
192
466
988
1878
3280
5362
8316
12358
send userid:4 subkey:28to server9010
send userid:4 subkey:70to server9011
send userid:4 subkey:192to server9012
send userid:4 subkey:466to server9013
send userid:4 subkey:988to server9014
send userid:4 subkey:1878to server9015
send userid:4 subkey:3280to server9016
send userid:4 subkey:5362to server9017
send userid:4 subkey:8316to server9018
send userid:4 subkey:12358to server9019
recvive98from pass_server
send userid:4to server9020
receive the subkey of userid=4:28from subserver:9020
send userid:4to server9021
receive the subkey of userid=4:70from subserver:9021
send userid:4to server9022
receive the subkey of userid=4:192from subserver:9022
send userid:4to server9023
receive the subkey of userid=4:466from subserver:9023
send userid:4to server9024
receive the subkey of userid=4:988from subserver:9024
send userid:4to server9025
receive the subkey of userid=4:1878from subserver:9025
send userid:4to server9026
receive the subkey of userid=4:3280from subserver:9026
send userid:4to server9027
receive the subkey of userid=4:5362from subserver:9027
send userid:4to server9028
receive the subkey of userid=4:8316from subserver:9028
send userid:4to server9029
receive the subkey of userid=4:12358from subserver:9029
real passwordid=18
userid:4,passwordid:18is correct!
recvive80from pass_server
send userid:4to server9020
receive the subkey of userid=4:28from subserver:9020
send userid:4to server9021
receive the subkey of userid=4:70from subserver:9021
```


C:\Users\dragon\Desktop\课程资料\2信息安全工程\项目\honeyword\checker_server\Debug\checker_server.exe
send userid:4to server9021
receive the subkey of userid=4:70from subserver:9021
send userid:4to server9022
receive the subkey of userid=4:192from subserver:9022
send userid:4to server9023
receive the subkey of userid=4:466from subserver:9023
send userid:4to server9024
receive the subkey of userid=4:988from subserver:9024
send userid:4to server9025
receive the subkey of userid=4:1878from subserver:9025
send userid:4to server9026
receive the subkey of userid=4:3280from subserver:9026
send userid:4to server9027
receive the subkey of userid=4:5362from subserver:9027
send userid:4to server9028
receive the subkey of userid=4:8316from subserver:9028
send userid:4to server9029
receive the subkey of userid=4:12358from subserver:9029
real passwordid=18
userid:4,passwordid:18is correct!
recvive80from pass_server
send userid:4to server9020
receive the subkey of userid=4:28from subserver:9020
send userid:4to server9021
receive the subkey of userid=4:70from subserver:9021
send userid:4to server9022
receive the subkey of userid=4:192from subserver:9022
send userid:4to server9023
receive the subkey of userid=4:466from subserver:9023
send userid:4to server9024
receive the subkey of userid=4:988from subserver:9024
send userid:4to server9025
receive the subkey of userid=4:1878from subserver:9025
send userid:4to server9026
receive the subkey of userid=4:3280from subserver:9026
send userid:4to server9027
receive the subkey of userid=4:5362from subserver:9027
send userid:4to server9028
receive the subkey of userid=4:8316from subserver:9028
send userid:4to server9029
receive the subkey of userid=4:12358from subserver:9029
real passwordid=18
userid:4,passwordid:0;warning!someone might get the password file!

C:\Users\dragon\Desktop\课程资料\2信息安全工程\项目\honeyword\distributed_server\Debug\distributed_server.exe

```
subserver:9011is processing!
subserver:9013is processing!
subserver:9014is processing!
subserver:9012is processing!
subserver:9019is processing!
subserver 9020is processing!
subserver 9025is processing!
subserver 9029is processing!
subserver:9015is processing!
subserver:9018is processing!
subserver 9027is processing!
subserver 9021is processing!
subserver 9023is processing!
subserver 9022is processing!
subserver:9017is processing!
subserver 9028is processing!
subserver 9024is processing!
subserver:9010is processing!
subserver 9026is processing!
subserver:9016is processing!
subserver9010receive userid:4subkey28from checker
4 28
subserver9011receive userid:4subkey70from checker
4 70
subserver9012receive userid:4subkey192from checker
4 192
subserver9013receive userid:4subkey466from checker
4 466
subserver9014receive userid:4subkey988from checker
4 988
subserver9015receive userid:4subkey1878from checker
4 1878
subserver9016receive userid:4subkey3280from checker
4 3280
subserver9017receive userid:4subkey5362from checker
4 5362
subserver9018receive userid:4subkey8316from checker
4 8316
subserver9019receive userid:4subkey12358from checker
4 12358
subserver9020receive userid:4from checker
subserver9020send the subkey of userid=4:28to checker
subserver9021receive userid:4from checker
subserver9021send the subkey of userid=4:70to checker
subserver9022receive userid:4from checker
subserver9022send the subkey of userid=4:192to checker
subserver9023receive userid:4from checker
subserver9023send the subkey of userid=4:466to checker
subserver9024receive userid:4from checker
subserver9024send the subkey of userid=4:988to checker
subserver9025receive userid:4from checker
subserver9025send the subkey of userid=4:1878to checker
```

选择C:\Users\dragon\Desktop\课程资料\2信息安全工程\项目\honeyword\distributed_server\Debug\distributed_server.exe

```
4 3280
subserver9017receive userid:4subkey5362from checker
4 5362
subserver9018receive userid:4subkey8316from checker
4 8316
subserver9019receive userid:4subkey12358from checker
4 12358
subserver9020receive userid:4from checker
subserver9020send the subkey of userid=4:28to checker
subserver9021receive userid:4from checker
subserver9021send the subkey of userid=4:70to checker
subserver9022receive userid:4from checker
subserver9022send the subkey of userid=4:192to checker
subserver9023receive userid:4from checker
subserver9023send the subkey of userid=4:466to checker
subserver9024receive userid:4from checker
subserver9024send the subkey of userid=4:988to checker
subserver9025receive userid:4from checker
subserver9025send the subkey of userid=4:1878to checker
subserver9026receive userid:4from checker
subserver9026send the subkey of userid=4:3280to checker
subserver9027receive userid:4from checker
subserver9027send the subkey of userid=4:5362to checker
subserver9028receive userid:4from checker
subserver9028send the subkey of userid=4:8316to checker
subserver9029receive userid:4from checker
subserver9029send the subkey of userid=4:12358to checker
subserver9020receive userid:4from checker
subserver9020send the subkey of userid=4:28to checker
subserver9021receive userid:4from checker
subserver9021send the subkey of userid=4:70to checker
subserver9022receive userid:4from checker
subserver9022send the subkey of userid=4:192to checker
subserver9023receive userid:4from checker
subserver9023send the subkey of userid=4:466to checker
subserver9024receive userid:4from checker
subserver9024send the subkey of userid=4:988to checker
subserver9025receive userid:4from checker
subserver9025send the subkey of userid=4:1878to checker
subserver9026receive userid:4from checker
subserver9026send the subkey of userid=4:3280to checker
subserver9027receive userid:4from checker
subserver9027send the subkey of userid=4:5362to checker
subserver9028receive userid:4from checker
subserver9028send the subkey of userid=4:8316to checker
subserver9029receive userid:4from checker
subserver9029send the subkey of userid=4:12358to checker
```