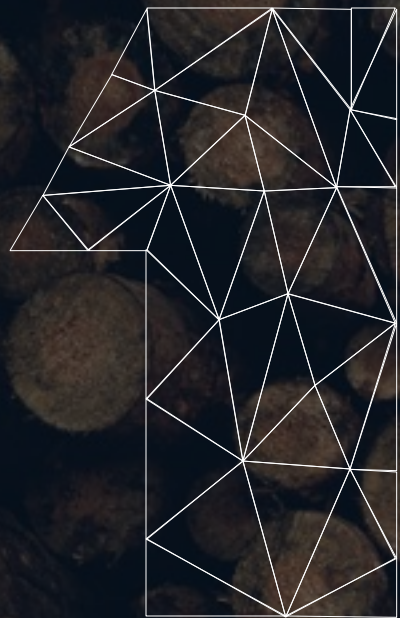




屏幕键盘安全性分析

-
- 14信安 许倩玉
 - 201411123002
-



PART ONE

写在前面



PART TWO

基础概念



PART THREE

试验过程



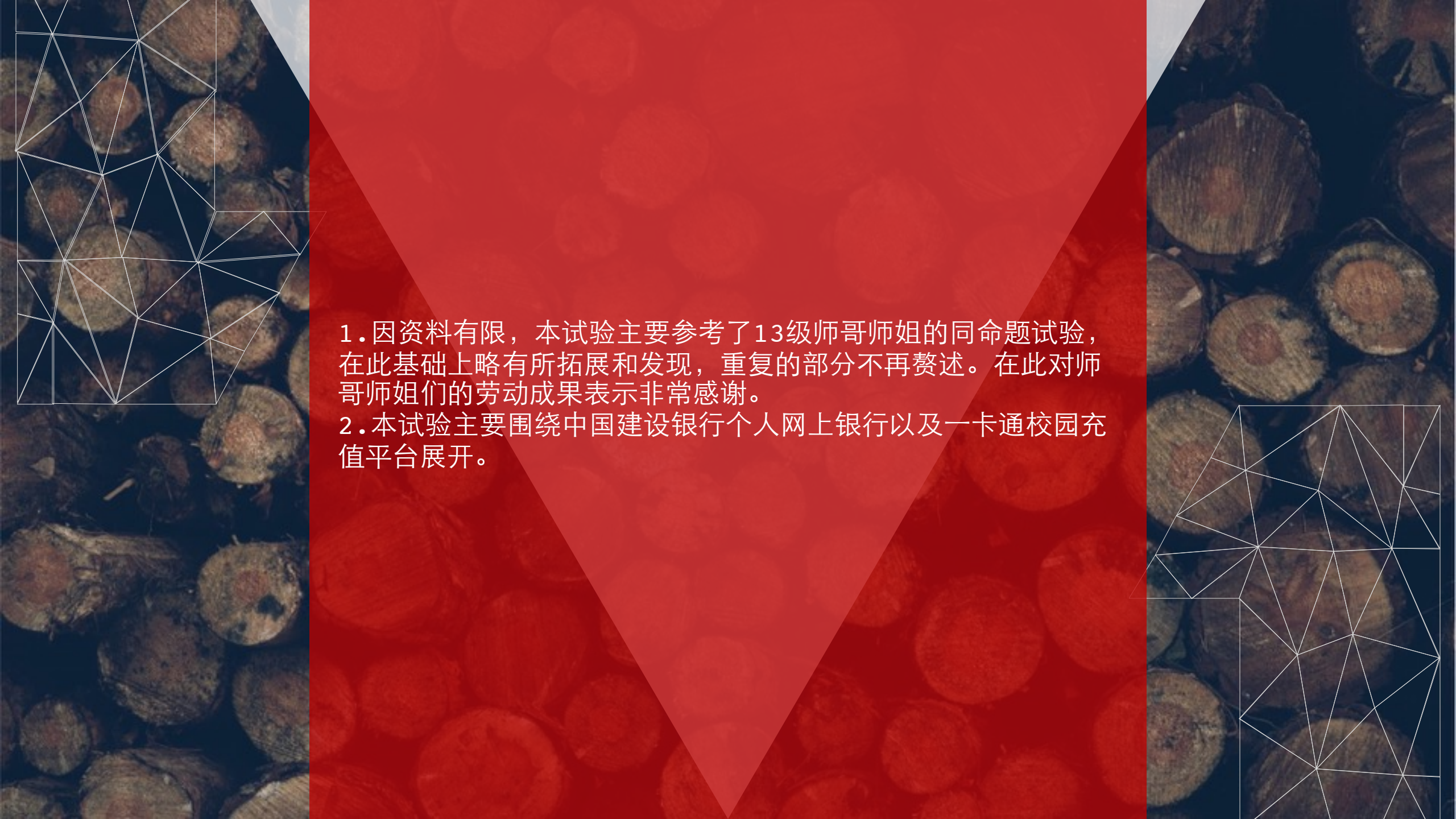
PART FOUR

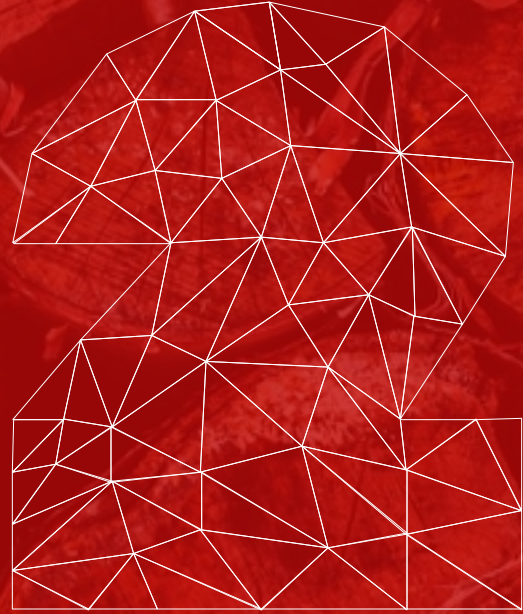
小结



PART ONE


写在前面

- 
1. 因资料有限，本试验主要参考了13级师哥师姐的同命题试验，在此基础上略有所拓展和发现，重复的部分不再赘述。在此对师哥师姐们的劳动成果表示非常感谢。
 2. 本试验主要围绕中国建设银行个人网上银行以及一卡通校园充值平台展开。



PART TWO

基本概念



http://wenku.baidu.com/link?url=x4uB1nDPdQiuZsvYh-Gm-plSljyBiap3KLvTxMlymz1l9Rqicl-lhnGL_7119WzBMP_MlxRBbkyyt7_0xBUUVLMSYPyHoUEiKf831s1xAm



PART THREE

试验过程



一卡通充值转账平台

实验环境：Google Chrome 55.0.2883.95 (64-bit) + Safari 10.0.1 [考虑到师哥师姐的实验环境也是Chrome浏览器，为了呈现不同实验环境下可能的不同结果，原本只选择了实验环境Safari 10.0.1，但是经过笔者在建行个人网银平台的一些尝试性操作后发现，找不到关键字段LOGPASS，而笔者的VPN最近又不太稳定，所以只好两个实验环境结合进行]

中国建设银行个人网上银行登录
https://ibsbjstar.ccb.com.cn/CCBIS/V6/common/login.jsp?UDC_CUSTOMER_ID=&UDC_CUSTOMER_NAME=&UDC_COOKIE=ddcd51b64719c89cwmloLt0QT6Z3YnF9m8YO1483266092289EtGwFLMeKc2Z92rSCNW8ed65098f1232918f52ea18c76e2158a&UDC_SESSION_ID=wb9HI9M1eLaShjg9822fe57867a-20170101182132

实验工具：Wireshark 2.0.3
[原本没有考虑到使用其他的实验工具，但是笔者的Chrome浏览器无法访问<https://ykt.cuc.edu.cn>，而Safari又无法从开发界面查看到Cookie的详细内容，因此想到了用Wireshark进行抓包查看]

校园卡电子服务平台
<http://ykt.cuc.edu.cn>



温馨提示：向校园卡转账成功后所转金额将显示在过渡余额中，在餐厅等处的卡机上进行刷卡操作后，过渡余额即会转入校园卡。单笔转账最大限额500元！

转账方式： 校园卡绑定银行卡 向 校园卡 转账

转账金额： RMB(单笔转账金额最大500)

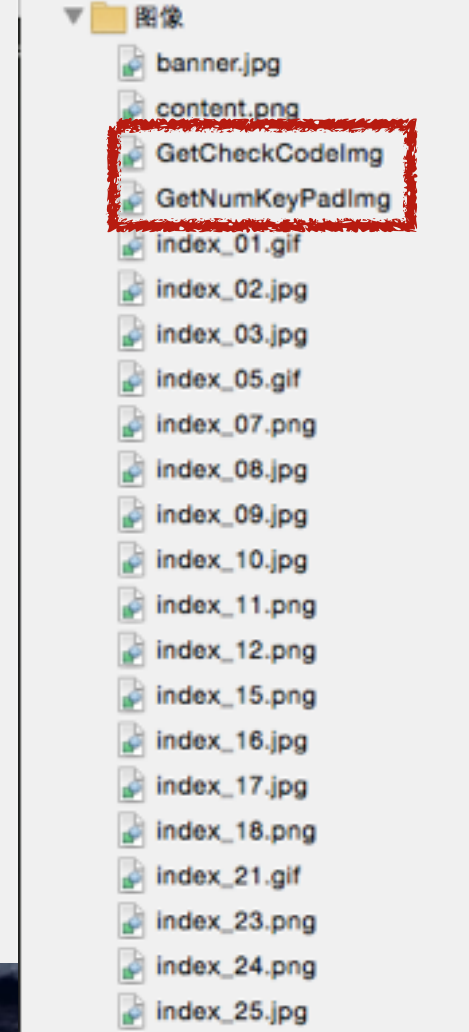
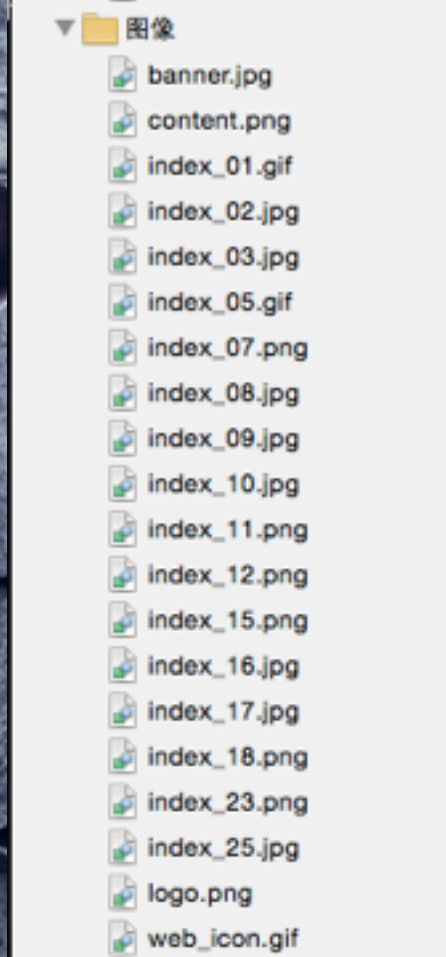
查询密码： *(校园卡查询密码)

6	2	0	1	4	5	7	8	3	9
退格	清空			确定					

验证码： *

3 3 6 6 看不清楚，换一张

☐ 我已阅读并同意缴费服务条款



登录<https://ykt.cuc.edu.cn>后，点击转账充值，会发现资源—>ykt.cuc.edu.cn—>图像列表中多出两个条目，其中的GetNumKeyPading即是当前屏幕键盘图。而相应的，充值界面的软键盘只有在页面刷新之后才会更新，而非每次输入刷新一次。


```
<label>␣  
    查询密码: </label>␣  
    <input type="password" id="Password" name="password" readonly="readonly" maxlength="6"␣  
        class="validate[required,minSize[6],maxSize[6]]" /><span class="red">*(校园卡查询密码)</span></p>␣  
<div class="virtualKey" id="password_key_transfer" style="display: none;">␣  
    ␣  
    <map name="keyboardMapForPwd" id="keyboardMapForPwd">␣  
        <area shape="rect" coords="4,3,29,28" value="0" />␣  
        <area shape="rect" coords="33,3,58,28" value="1" />␣  
        <area shape="rect" coords="62,3,88,28" value="2" />␣  
        <area shape="rect" coords="92,3,118,28" value="3" />␣  
        <area shape="rect" coords="122,3,148,28" value="4" />␣  
        <area shape="rect" coords="152,3,178,28" value="5" />␣  
        <area shape="rect" coords="182,3,207,28" value="6" />␣  
        <area shape="rect" coords="211,3,236,28" value="7" />␣  
        <area shape="rect" coords="241,3,266,28" value="8" />␣  
        <area shape="rect" coords="270,3,295,28" value="9" />␣  
        <area shape="rect" coords="5,33,74,148" value="Backspace" />␣  
        <area shape="rect" coords="78,33,221,148" value="Clear" />␣  
        <area shape="rect" coords="227,33,295,148" value="Close" />␣  
    </map>␣  
</div>␣
```

资源—>ykt.cuc.edu.cn—>XHR—>Transfer，找到如上图所示代码，coords表示坐标，而从代码中来看，键盘的坐标似乎是固定的。笔者尝试刷新过几次页面，此段代码并没有改变。而通过前文中可知，键盘的图片又是随着刷新而变化的，因此猜想是否学校的服务器存在某个图片库，每次刷新的时候都向该服务器请求了新的键盘图片？而无论图片上的数字如何分布，实际键盘上的输入总是按照 0~9 排列？为此，笔者进行了数次如下尝试。

键盘序列：6201457839

操作：维持上述键盘序列，不刷新页面，多次输入执行转账操作，每次点击“立即转账”之前清空缓存，同时用Wireshark开始抓包。



实验次序	键盘序列	输入密码	POST包中加密密码
1	6201457839	620145	543210
2	6201457839	620145	543210
3	6201457839	662200	221100
4	6201457839	220011	332211
5	6201457839	001114	443332

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
41	4.447724	10.194.25.31	202.205.25.18	HTTP	547	GET /Content/t...
42	4.447926	10.194.25.31	202.205.25.18	HTTP	551	GET /Content/t...
45	4.462329	202.205.25.18	10.194.25.31	HTTP	413	HTTP/1.1 200 O...
49	4.471671	10.194.25.31	202.205.25.18	HTTP	551	GET /Content/t...
51	4.472298	202.205.25.18	10.194.25.31	HTTP	491	HTTP/1.1 200 O...
56	4.482945	10.194.25.31	202.205.25.18	HTTP	551	GET /Content/t...
57	4.509326	202.205.25.18	10.194.25.31	HTTP	424	HTTP/1.1 200 O...
63	4.527478	202.205.25.18	10.194.25.31	HTTP	423	HTTP/1.1 200 O...
67	4.879026	202.205.25.18	10.194.25.31	HTTP	491	[TCP Spurious ...
71	6.022351	10.194.25.31	202.205.25.18	HTTP	551	GET /Content/t...
73	6.038028	10.194.25.31	202.205.25.18	HTTP	148	POST /CardMana...
84	9.564664	202.205.25.18	10.194.25.31	HTTP	358	HTTP/1.1 200 O...
86	9.590061	10.194.25.31	202.205.25.18	HTTP	535	GET /Account/G...
100	11.918710	202.205.25.18	10.194.25.31	HTTP	418	HTTP/1.1 200 O...
105	13.379936	10.194.25.31	202.205.25.18	HTTP	550	GET /Content/t...
106	13.385036	202.205.25.18	10.194.25.31	HTTP	493	HTTP/1.1 200 O...

\r\n
[\[Full request URI: http://ykt.cuc.edu.cn/CardManage/CardInfo/TransferAccount\]](http://ykt.cuc.edu.cn/CardManage/CardInfo/TransferAccount)
 [HTTP request 2/3]
[\[Prev request in frame: 41\]](#)
[\[Response in frame: 84\]](#)
[\[Next request in frame: 86\]](#)

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

- ▶ Form item: "password" = "543210"
- ▶ Form item: "checkCode" = "3366"
- ▶ Form item: "amt" = "100.00"
- ▶ Form item: "fcard" = "bcard"
- ▶ Form item: "tocard" = "card"
- ▶ Form item: "bankno" = ""
- ▶ Form item: "bankpwd" = ""

```

0000  00 00 5e 00 01 b5 2c f0 ee 30 9e 1a 08 00 45 00  ..^.... .0....E.
0010  00 86 99 8b 40 00 40 06 99 26 0a c2 19 1f ca cd  ....@.@. .&.....
0020  19 12 c3 9f 00 50 c5 6f 8c dd e2 f2 09 e5 00 18  ....P.o .....
0030  10 00 d7 08 00 00 01 01 08 0a 01 23 a5 64 1f 41  .... .#.d.A
0040  88 87 70 61 73 73 77 6f 72 64 3d 35 34 33 32 31  ..passwo rd=54321
0050  30 26 63 68 65 63 6b 43 6f 64 65 3d 33 33 36 36  0&checkC ode=3366
  
```

Frame (148 bytes) Reassembled TCP (679 bytes)

wireshark_pcapng_en0_20170103003333_u9NAV2 Packets: 107 · Displayed: 17 (15.9%) Profile: Default

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
592	3.792722	220.181.90.12	10.194.25.31	HTTP	979	HTTP/1.1 404 Not...
594	3.795804	10.194.25.31	220.181.90.12	HTTP	273	GET /favicon.ico...
595	3.804448	220.181.90.12	10.194.25.31	HTTP	1365	HTTP/1.1 200 OK ...
597	3.811175	10.194.25.31	220.181.90.12	HTTP	483	GET / HTTP/1.1
598	3.818719	220.181.90.12	10.194.25.31	HTTP	467	HTTP/1.1 302 Mov...
615	3.884971	10.194.25.31	220.181.90.52	HTTP	456	GET /c/18159/?_t...
633	3.966074	10.194.25.31	220.181.20.130	HTTP	291	GET /apple-touch...
653	4.026327	10.194.25.31	59.151.11.19	HTTP	398	GET / HTTP/1.1
655	4.094975	59.151.11.19	10.194.25.31	HTTP	674	HTTP/1.1 302 Mov...
663	4.133984	10.194.25.31	202.205.25.18	HTTP	148	POST /CardManage...
668	4.205700	202.205.25.18	10.194.25.31	HTTP	432	HTTP/1.1 200 OK ...
670	4.226793	10.194.25.31	202.205.25.18	HTTP	459	GET /Account/Get...
763	5.038529	10.194.25.31	59.151.11.19	HTTP	445	GET / HTTP/1.1
781	5.092484	59.151.11.19	10.194.25.31	HTTP	688	HTTP/1.1 302 Mov...
807	5.129788	10.194.25.31	120.132.34.26	HTTP	460	GET /?bd_source=...
893	5.332933	10.194.25.31	118.187.1.104	HTTP	281	GET /apple-touch...
893	5.438034	120.132.34.26	10.194.25.31	HTTP	803	HTTP/1.1 200 OK ...

X-Requested-With: XMLHttpRequest\r\n\r\n

[Full request URI: <http://ykt.cuc.edu.cn/CardManage/CardInfo/TransferAccount>]

[HTTP request 1/2]

[Response in frame: 668]

[Next request in frame: 670]

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "password" = "543210"
- Form item: "checkCode" = "8782"
- Form item: "amt" = "100.00"
- Form item: "fcard" = "bcard"
- Form item: "tocard" = "card"
- Form item: "bankno" = ""
- Form item: "bankpwd" = ""

```

0000  00 00 5e 00 01 b5 2c f0 ee 30 9e 1a 08 00 45 00  ..^..... .0....E.
0010  00 06 55 d2 40 00 40 06 dc df 0a c2 19 1f ca cd  ..U.@. ....
0020  19 12 c5 1f 00 50 75 3c dd 22 3f 36 c0 a9 80 18  ....Pu< ."76....
0030  10 15 fd 82 00 00 01 01 08 0a 01 27 0a c8 1f 41  ....'...A
0040  e0 f6 70 61 73 73 77 6f 72 64 3d 35 34 33 32 31  ..passwo rd=54321
0050  30 26 63 68 65 63 6b 43 6f 64 65 3d 38 37 38 32  0&checkC ode=8782

```

Frame (148 bytes) Reassembled TCP (551 bytes)

wireshark_pcapng_en0_20170103003720_pNUR6X Packets: 1764 - Displayed: 56 (3.2%) Profile: Default

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
441	3.096220	10.194.25.31	175.25.168.45	HTTP	462	GET /travels/inf...
450	3.203284	175.25.168.45	10.194.25.31	HTTP	60	HTTP/1.1 302 Mov...
465	3.220534	10.194.25.31	175.25.168.45	HTTP	464	GET /m/travels/i...
476	3.550380	10.194.25.31	175.25.168.45	HTTP	554	GET /apple-touch...
486	3.669592	175.25.168.45	10.194.25.31	HTTP	515	HTTP/1.1 200 OK ...
488	3.672416	10.194.25.31	175.25.168.45	HTTP	542	GET /apple-touch...
495	3.779497	10.194.25.31	175.25.168.45	HTTP	533	GET /favicon.ico...
504	3.896679	175.25.168.45	10.194.25.31	HTTP	318	[TCP Spurious Re...
511	3.932787	10.194.25.31	114.80.165.233	HTTP	409	GET /citylist HT...
516	3.985899	10.194.25.31	202.205.25.18	HTTP	148	POST /CardManage...
518	4.004800	202.205.25.18	10.194.25.31	HTTP	432	HTTP/1.1 200 OK ...
520	4.037902	10.194.25.31	202.205.25.18	HTTP	459	GET /Account/Get...
597	4.248427	10.194.25.31	114.80.165.233	HTTP	402	GET /apple-touch...
599	4.292063	114.80.165.233	10.194.25.31	HTTP	607	HTTP/1.1 302 Fou...
601	4.294353	10.194.25.31	114.80.165.233	HTTP	370	GET / HTTP/1.1
602	4.366737	114.80.165.233	10.194.25.31	HTTP	295	HTTP/1.1 302 Fou...
604	4.369342	10.194.25.31	114.80.165.233	HTTP	370	GET /citylist HT...

X-Requested-With: XMLHttpRequest\r\n\r\n

[Full request URI: <http://ykt.cuc.edu.cn/CardManage/CardInfo/TransferAccount/>]

[HTTP request 1/2]

[Response in frame: 518]

[Next request in frame: 520]

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "password" = "221100"
- Form item: "checkCode" = "5595"
- Form item: "amt" = "100.00"
- Form item: "fcard" = "bcard"
- Form item: "tocard" = "card"
- Form item: "bankno" = ""
- Form item: "bankpwd" = ""

```

0000  00 00 5e 00 01 b5 2c f0 ee 30 9e 1a 08 00 45 00  ..^.... .0....E.
0010  00 86 35 5d 40 00 40 06 fd 54 0a c2 19 1f ca cd  ..5]@.@. .T.....
0020  19 12 c6 7b 00 50 7b bb bb 64 c3 07 78 84 00 18  ...{.P{. .d..x...
0030  10 00 c0 03 00 00 01 01 08 0a 01 29 f4 49 1f 42  .... .I.B
0040  18 42 70 61 73 77 6f 72 64 3d 32 32 31 31 30    .Bpasswo rd=22110
0050  30 26 63 68 65 63 6b 43 6f 64 65 3d 35 35 39 35  0&checkC ode=5595

```

Frame (148 bytes) Reassembled TCP (551 bytes)

wireshark_pcapng_en0_20170103004034_HsPONu Packets: 956 · Displayed: 74 (7.7%) Profile: Default

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
14	0.714611	23.23.204.240	10.194.25.31	HTTP	1514	[TCP Fast Retran...
17	0.725701	10.194.25.31	23.23.204.240	HTTP	337	GET /static/imag...
31	2.073180	10.194.25.31	103.233.81.78	HTTP	414	GET /member/buy...
33	2.169954	103.233.81.78	10.194.25.31	HTTP	462	HTTP/1.1 301 Mov...
86	3.282020	10.194.25.31	202.205.25.18	HTTP	148	POST /CardManage...
88	3.305454	202.205.25.18	10.194.25.31	HTTP	352	HTTP/1.1 200 OK ..
90	3.324641	10.194.25.31	202.205.25.18	HTTP	459	GET /Account/Get...
133	4.420192	10.194.25.31	103.233.81.78	HTTP	461	GET /member/buy...
135	4.518701	103.233.81.78	10.194.25.31	HTTP	462	HTTP/1.1 301 Mov...

Cookie pair: ASP.NET_SessionId=eyjo30llgarbmr5oyayh5kvv
 \r\n
[\[Full request URI: http://ykt.cuc.edu.cn/CardManage/CardInfo/TransferAccount\]](http://ykt.cuc.edu.cn/CardManage/CardInfo/TransferAccount)
 [HTTP request 1/2]
[\[Response in frame: 88\]](#)
[\[Next request in frame: 90\]](#)

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

- Form item: "password" = "332211"
- Form item: "checkCode" = "1126"
- Form item: "amt" = "100.00"
- Form item: "fcard" = "bcard"
- Form item: "tocard" = "card"
- Form item: "bankno" = ""
- Form item: "bankpwd" = ""

0000 00 00 5e 00 01 b5 2c f0 ee 30 9e 1a 08 00 45 00 ..^..... .0....E.
 0010 00 06 eb 42 40 00 40 06 47 6f 0a c2 19 1f ca cd ...B@.@. Go.....
 0020 19 12 c7 a3 00 50 9e dc 8b de 5b d9 19 0e 00 18P.. ..[.....
 0030 10 15 ef 5d 00 00 01 01 08 0a 01 2c 4d 8f 1f 42 ...].... ...,M..B
 0040 69 6c 70 61 73 73 77 6f 72 64 3d 33 33 32 32 31 ilpasswo rd=33221
 0050 31 26 63 68 65 63 6b 43 6f 64 65 3d 31 31 32 36 1&checkC ode=1126

Frame (148 bytes) Reassembled TCP (603 bytes)

wireshark_pcapng_en0_20170103004310_57XkM4 Packets: 254 - Displayed: 9 (3.5%) Profile: Default

Wi-Fi: en0

http

No.	Time	Source	Destination	Protocol	Length	Info
7	0.018418	10.194.25.31	202.205.25.18	HTTP	148	POST /CardManage...
9	0.049846	202.205.25.18	10.194.25.31	HTTP	352	HTTP/1.1 200 OK
11	0.069130	10.194.25.31	202.205.25.18	HTTP	459	GET /Account/Get...

Cookie pair: ASP.NET_SessionId=eyjo30llgarbmr5oyayh5kvv
\r\n
[\[Full request URI: http://ykt.cuc.edu.cn/CardManage/CardInfo/TransferAccount\]](http://ykt.cuc.edu.cn/CardManage/CardInfo/TransferAccount)
[HTTP request 1/2]
[\[Response in frame: 9\]](#)
[\[Next request in frame: 11\]](#)

▼ HTML Form URL Encoded: application/x-www-form-urlencoded

- ▶ Form item: "password" = "443332"
- ▶ Form item: "checkCode" = "4276"
- ▶ Form item: "amt" = "100.00"
- ▶ Form item: "fcard" = "bcard"
- ▶ Form item: "tocard" = "card"
- ▶ Form item: "bankno" = ""
- ▶ Form item: "bankpwd" = ""

```

0000  00 00 5e 00 01 b5 2c f0 ee 30 9e 1a 08 00 45 00  ..^.... .0....E.
0010  00 86 4c ad 40 00 40 06 e6 04 0a c2 19 1f ca cd  ..L.@. ....
0020  19 12 c7 bb 00 50 85 e5 87 dc 6d ed 56 f8 80 18  ....P.. ..m.V...
0030  10 15 5e ff 00 00 01 01 08 0a 01 2e 69 a9 1f 42  ..^..... ..i..B
0040  9f 8c 70 61 73 73 77 6f 72 64 3d 34 34 33 33 33  ..passwo rd=44333
0050  32 26 63 68 65 63 6b 43 6f 64 65 3d 34 32 37 36  2&checkC ode=4276

```

Frame (148 bytes) Reassembled TCP (603 bytes)

wireshark_pcapng_en0_20170103004522_55fhOV Packets: 17 - Displayed: 3 (17.6%) Profile: Default

实验次序	键盘序列	输入密码	POST包中加密密码
1	6201457839	620145	543210
2	6201457839	620145	543210
3	6201457839	662200	221100
4	6201457839	220011	332211
5	6201457839	001114	443332

由该表分析可知：

- 1.如果维持同一屏幕键盘，输入同样的密码，则得到相同的加密密码，由此可证明密码加密算法随机性较低。
- 2.虽然密码和加密密码中存在某些反转调整，比如试验3中6→2，2→1，0→0，试验5中0→4，1→3，4→2，但是元素的个数都是一一对应的，依然具有可统计性。



中国建设银行个人网银登陆平台

登录个人网上银行

 用户名/证件号码

 登录密码

软键盘

登 录

☐ 记住用户名

[忘记密码](#) | [忘记密码](#)

未开通网上银行? [马上开通](#)

中国建设银行 密码输入器													使用键盘输入	
~	!	@	#	\$	%	^	&	*	()	-	+		退格
`	6	1	9	3	2	5	4	8	7	0	_	=	\	空格
t	q	u	r	i	w	y	e	o	p	{	}	[]	切换大小写
a	f	d	g	s	h	j	k	l	:	;	"	'	确定	
z	x	b	v	c	n	m	<	,	>	.	?	/		

中国建设银行 密码输入器														使用键盘输入
~	!	@	#	\$	%	^	&	*	()	-	+		退格
`	2	0	1	6	4	3	5	7	8	9	_	=	\	空格
u	o	i	w	t	y	e	r	q	p	{	}	[]	切换大小写
g	l	d	h	k	f	j	s	a	:	;	"	'	确定	
z	x	n	v	b	c	m	<	,	>	.	?	/		

中国建设银行 密码输入器													使用键盘输入	
~	!	@	#	\$	%	^	&	*	()	-	+		退格
`	8	9	2	4	1	3	6	5	7	0	_	=	\	空格
e	w	q	r	y	i	p	t	o	u	{	}	[]	切换大小写
a	s	l	g	j	h	d	k	f	:	;	"	'	确定	
c	z	m	v	b	x	n	<	,	>	.	?	/		

中国建设银行 密码输入器													使用键盘输入	
~	!	@	#	\$	%	^	&	*	()	-	+		退格
`	1	6	0	3	8	5	4	7	2	9	_	=	\	空格
e	w	y	p	q	t	u	r	i	o	{	}	[]	切换大小写
g	s	a	k	d	f	j	h	l	:	;	"	'	确定	
v	z	c	m	b	n	x	<	,	>	.	?	/		

中国建设银行 密码输入器													使用键盘输入	
~	!	@	#	\$	%	^	&	*	()	-	+		退格
`	6	1	2	9	4	5	3	7	8	0	_	=	\	空格
i	w	t	o	q	y	u	r	p	e	{	}	[]	切换大小写
k	s	l	d	g	h	j	a	f	:	;	"	'	确定	
n	x	v	z	b	c	m	<	,	>	.	?	/		

中国建设银行 密码输入器													使用键盘输入	
~	!	@	#	\$	%	^	&	*	()	-	+		退格
`	4	1	3	2	8	0	6	5	7	9	_	=	\	空格
o	r	w	y	t	q	e	u	p	i	{	}	[]	切换大小写
l	f	h	s	g	j	k	a	d	:	;	"	'	确定	
v	n	b	z	c	x	m	<	,	>	.	?	/		

中国建设银行 密码输入器													使用键盘输入	
~	!	@	#	\$	%	^	&	*	()	-	+		退格
`	6	7	2	3	0	5	4	8	9	1	_	=	\	空格
u	i	p	r	o	y	w	t	q	e	{	}	[]	切换大小写
a	s	j	l	g	h	f	k	d	:	;	"	'	确定	
v	x	m	c	b	z	n	<	,	>	.	?	/		

中国建设银行 密码输入器													使用键盘输入	
~	!	@	#	\$	%	^	&	*	()	-	+		退格
`	1	7	2	3	0	8	6	9	4	5	_	=	\	空格
i	q	p	r	w	y	u	t	o	e	{	}	[]	切换大小写
g	s	d	h	a	k	j	f	l	:	;	"	'	确定	
c	x	v	m	b	n	z	<	,	>	.	?	/		

中国建设银行 密码输入器														使用键盘输入
~	!	@	#	\$	%	^	&	*	()	-	+		退格
`	7	5	8	1	4	3	6	2	0	9	_	=	\	空格
t	p	e	r	y	w	u	q	o	i	{	}	[]	切换大小写
l	s	a	j	k	h	g	d	f	:	;	"	'	确定	
n	v	c	m	b	z	x	<	,	>	.	?	/		

中国建设银行 密码输入器													使用键盘输入	
~	!	@	#	\$	%	^	&	*	()	-	+		退格
`	0	2	1	4	6	5	3	7	8	9	_	=	\	空格
p	w	u	r	t	y	e	i	o	q	{	}	[]	切换大小写
g	j	d	f	l	k	a	s	h	:	;	"	'	确定	
z	c	x	v	b	n	m	<	,	>	.	?	/		

软键盘10次刷新截图


```

/*随机排序*/
function randomSord() {
    var arrayNums = [0, 1, 2, 3, 4, 5, 6, 7, 8, 9];
    var arrayLists1 = ["q", "w", "e", "r", "t", "y", "u", "i", "o", "p"];
    var arrayLists2 = ["a", "s", "d", "f", "g", "h", "j", "k", "l"];
    var arrayLists3 = ["z", "x", "c", "v", "b", "n", "m"];

    for (var i = 0; i < arrayNums.length; i++) {
        var randomNum = parseInt(Math.random() * 10) % arrayNums.length;
        var tmp = arrayNums[0];
        arrayNums[0] = arrayNums[randomNum];
        arrayNums[randomNum] = tmp;
    };

    for (var i = 0; i < arrayLists1.length; i++) {
        var randomNum = parseInt(Math.random() * 10) % arrayLists1.length;
        var tmp = arrayLists1[0];
        arrayLists1[0] = arrayLists1[randomNum];
        arrayLists1[randomNum] = tmp;
    };

    for (var i = 0; i < arrayLists2.length; i++) {
        var randomNum = parseInt(Math.random() * 10) % arrayLists2.length;
        var tmp = arrayLists2[0];
        arrayLists2[0] = arrayLists2[randomNum];
        arrayLists2[randomNum] = tmp;
    };

    for (var i = 0; i < arrayLists3.length; i++) {
        var randomNum = parseInt(Math.random() * 10) % arrayLists3.length;
        var tmp = arrayLists3[0];
        arrayLists3[0] = arrayLists3[randomNum];
        arrayLists3[randomNum] = tmp;
    };

    $(".tr_second td.random").each(function (index, element) {
        $(this).find("span").text(arrayNums[index]);
    });

    $(".tr_third td.random").each(function (index, element) {
        $(this).find("span").text(arrayLists1[index]);
    });

    $(".tr_fourth td.random").each(function (index, element) {
        $(this).find("span").text(arrayLists2[index]);
    });

    $(".tr_fifth td.random").each(function (index, element) {
        $(this).find("span").text(arrayLists3[index]);
    });
};
randomSord();
});
};

```

由10次刷新的软键盘截图可知，建行个人网银的用户登录密码输入键盘是随机自绘键盘，但是只有0~9十个数字以及a~z二十六个英文字母是随机分布的，其他的字符位置都是固定的。

打开中国建设银行个人客户网上银行页面后，打开开发者工具，在资源列表里top→fclogin(B2CMainPlat_00)→ibsbjstar.ccb.com.cn→P1StaRes/V6/STY1/CN→js中找到一个名为“softkeyboard”的js文件。通过阅读分析代码可知，中国建设银行个人网银登陆界面的虚拟键盘共有三种格式：虚拟数字键盘、虚拟键盘、增强版虚拟数字键盘。

其中虚拟键盘的相应部分代码如图所示。

[illegible]

[illegible]

user	软键盘数字排列	输入密码	CCB_PWD_MAP_GIGEST	加密后密码
a	1234597860	111111	28433853633))))))
a	1260573894	111111	28433853633))))))
a	1845607392	111111	28434001131	yyyyyy
b	1234860975	111111	28434001131	yyyyyy
b	1298765304	111111	28434060707	zzzzzz

<i>user</i>	<i>password</i>	<i>CCB_PWD_MAP_GIGEST</i>	<i>LOGPASS</i>
xqy	111111	S000000344109136ILOGPASS	777777
xqy	111111	S000000344109910ILOGPASS	nnnnnnn
xjd	111111	S000000343385271ILOGPASS	lllllll
xjd	111111	S000000344717678ILOGPASS	{{{{{{}}

经过了一系列数据测试，对比师哥师姐之前的实验结果截图（上表）可以发现，CCB_PWD_MAP_GIGEST字段的格式有了明显的变化，并且即使是连续不间断刷新输入用户名和密码登录，每一次得到的CCB_PWD_MAP_GIGEST字段的值和LOGPASS都不同，猜想可能提升了算法，为利用CCB_PWD_MAP_GIGEST字段值和LOGPASS字段值的更新时间差进行统计攻击增添了难度。



PART FOUR

小结

一卡通充值转账平台

1. 加密算法随机较差，需要定期提升完善。
2. 屏幕键盘刷新闻隔较长，最好应实现每次输入刷新一次。
3. 没有输入密码错误次数限制，最好有所管制，例如设定在3~5次左右。

建行个人网银登陆平台

1. 加密算法经过改善后随机性较好，即便输入的密码相同得到的加密密码也不相同。
2. 即便不刷新页面，每次输入时的屏幕键盘也不相同。
3. 有错误限制次数。
4. 密码输入依然保留了物理键盘输入，存在风险。

总而言之，一卡通充值转账平台安全性较低，即便作为用户在每次输入密码时刷新一下页面，但如果被有心人破解了加密算法，亦是无用。相对来说，建行个人网银登陆平台安全性较高，但是保留物理键盘输入仍然存在风险。而二者是否都存在被截屏攻击的风险因技术限制尚不得而知。



THE END