NSFOCUS

Personal Internet banking login security research report

个人网上银行登录安全研究报告

NSFOCUS

赵粮
绿盟科技 NSFOCUS
首席战略官 CSO

A. 序言

亲爱的读者：

2013 年初，绿盟科技专业服务的同事们对中国银行业个人网上银行的登录安全进行了一项专题研究。中国 50 大银行、4 个独特的角度、12 个令人印象深刻的观点，构成了这份研究报告的主要轮廓。

网上银行用户选择使用什么认证方式？这些认证方式安全性怎么样？SSL 安全吗？网上银行常用的安全控件有效吗？对不同浏览器的支持怎么样？…如果您同样在思索这些问题，您会发现这份报告非常值得一读。

绿盟科技在中国已经走过 13 年，专业安全服务一直是绿盟科技最为重要的一个业务领域。在多年为银行客户提供专业服务的过程中，积累了对个人网上银行安全性的深入理解。这份报告是这些理解的一个分享。

希望您阅读愉快，对您有所启发。

赵粮
绿盟科技首席战略官

B. 执行摘要

2013 年初，绿盟科技专业服务的同事们对中国银行业个人网上银行的登录安全进行了一项专题研究。

我们根据 2012 年 10 月 24 日标准普尔在北京发布的《中国 50 大银行》报告，对这 50 大银行的个人网上银行登录进行了调查、分析和深入研究，借此来巩固并完善我们在“入口安全”领域的安全积累。

通过此项研究，我们了解了当前中国 50 大银行个人网上银行业务中的登录安全现状，掌握了当前与登录安全相关的第一手宝贵资料。同时，我们也希望借助此项研究，总结经验，将其反馈给中国各大银行，为中国银行业网上银行的信息安全事业，尽我们的一份微薄之力；为推动中国银行业网上银行整体安全持续、健康、稳定的发展，做出我们的一份贡献。

我们是巨人背后的专家，我们甘为孺子牛。

有关个人网上银行登录安全研究的主要发现：

现状：安全措施日益多样，且细节丰富

1. 安全的 SSL 会话是网上银行登录的第一道防线
2. 多因素认证的身份鉴别方式已经得到普及
3. 对密码的输入保护多采用安全控件集成软键盘的混合模式
4. 验证码依然是登录中不可避免的负面体验
5. 登录失败策略差异较大，但反馈信息多使用“友好的错误提示”并进行了模糊化处理
6. 少数银行对客户端的浏览器要求更精细
7. 预留信息的作用并不明显
8. 欢迎首页的登录提醒信息多种多样
9. 与登录相关的限制策略应用百花齐放、百家争鸣，但效果不佳

攻与防：解决最突出的五大威胁是保障网上银行登录安全的关键

10. 网络钓鱼是个人网上银行登录最大的安全威胁
11. 恶意代码攻击与网上银行登录紧密相关
12. 暴力破解攻击在逐步降低，但仍不可忽视
13. 登录中的恶意滥用问题尚无非常有效的解决办法
14. 用户身份假冒是当前登录面临的最头痛问题

监管：合规不是终点而是起点，不要输在起跑线

15. 加密通信协议已经普及，弱加密算法尚存
16. 安全控件及软键盘广泛使用，但技术细粒度有待加强
17. 图形验证码安全合规性不容乐观

局限性：技术也有不足，得与失都得自己承担

18. 利用 USBKEY 证书的登录身份鉴别，也有硬伤
19. 安全控件是攻与防博弈的矛盾体
20. 验证码让用户慢下来，影响输入体验

C. 对象、范围和方法

对象

此项研究中，我们选取标准普尔发布的《中国 50 大银行》报告中的 50 大银行之个人网上银行为研究对象。

范围

此项研究中，我们将个人网上银行的登录作为安全研究专题，主要从登录安全中的不同角色关注的不同内容出发。分别从“现状：安全措施的真实情况”、“攻与防：最突出的安全威胁及应对”、“监管：合规要求和实现”和“局限性：技术的缺陷”四个核心主题进行安全探讨。

由于个人网上银行业务的独特性，我们没有把登录相关的“找回用户名”、“忘记密码”或“重置密码”等内容纳入到此项研究范围，请读者谅解。

方法

我们首先收集了绿盟科技各部门安全专家、顾问和工程师关于网上银行、支付网站的数百个登录相关的安全观点，对这些观点进行了筛选、合并、分类和排序，初步形成了若干个登录安全假设。

随后，我们研究了各银行个人网上银行的一系列资源来验证这些假设，包括亲身实践个人网上银行业务，查阅网上银行的演示、指导手册、安全指引等，以及一系列其他资料，包括学术文献、研究报告、互联网个人分析等。

通过上述验证过程，我们最终得出了若干个最有理有据的假设，由此融合成《个人网上银行登录安全研究报告》中所总结的四个核心主题，二十个子主题。

目录

D. 安全研究

D1. 现状：安全措施日益多样，且细节丰富

现在，转换您的身份，从一位本报告的阅读者变成网上银行用户的角色，来看一看当前我国各银行个人网上银行的登录安全，看看都采用了哪些安全防护措施来保障登录，解决登录过程的安全风险。

从您打开网上银行界面到成功进入网上银行欢迎页，或许您能发现下面这些安全措施：安全会话、身份鉴别、输入保护、验证码、失败处理、浏览器功能屏蔽、预留信息、登录提醒、限制策略。如果您都了解上述这些专业词汇，恭喜您，您不仅是一位敏锐的观察者，一定也是一位安全意识极高的网上银行忠实用户。

1）安全的 SSL 会话是网上银行登录的第一道防线

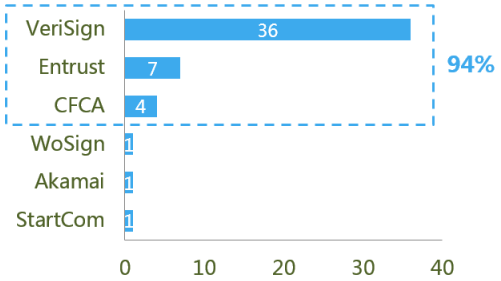
创建会话是用户与银行个人网上银行之间交互的第一步，没有安全的会话，个人网上银行的安全无从谈起。

基于我们对 50 大银行登录会话安全的调查数据和分析，结果显示：被调研的所有个人网上银行的网络通讯均采用 HTTPS 方式，应用安全套接字层（SSL）来确保建立一个安全的信道。

研究显示：国内银行更容易接受 VeriSign 颁发的 SSL 证书，除 VeriSign 外，Entrust、CFCA 也是常见的证书颁发机构。证书公钥普遍采用 RSA（2048Bits）公钥，也有少数采用 RSA（1024Bits）公钥的情况。证书有效期多集中在 24-27 个月之间，也有部分短期证书例如 9 个月。值得一提的是：在我们的调查中发现，少数银行的个人网上银行 SSL 证书信息存在异常状态，如：证书过期、证书颁发的域名与实际域名不匹配等。（见图 D.1.1）

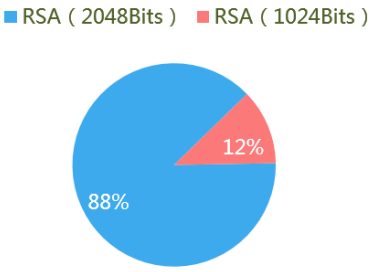
D.1.1 对安全的SSL会话的认知

VeriSign是最容易接受的SSL证书颁发机构,[%]



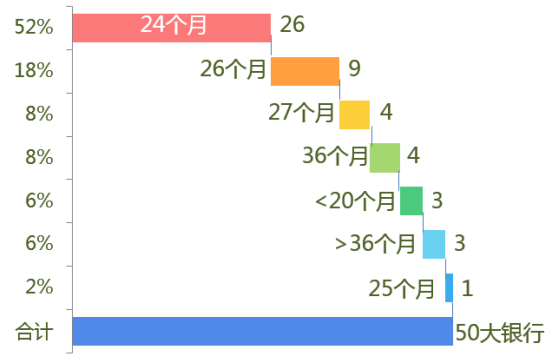
备注：数据样本为中国50大银行。
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

最普遍采用的SSL证书公钥是RSA（2048Bits）



备注：数据样本为中国50大银行。
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

过半数SSL证书颁发的有效期是二年,[%]



备注：数据样本为中国50大银行。
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

“SSL 通常是安全可靠的，但有两点可使 SSL 的安全性大大降低以至不可接受：一是不应该支持低强度对称加密算法，弱加密可使辛苦建立的会话密钥轻易被破解；二是数字证书的公私钥对不能可猜测。”

——绿盟科技 项目经理 李海涛

2）多因素认证的身份鉴别方式已经得到普及

网上银行用户的身份鉴别是各个银行个人网上银行业务安全的关键，正确识别和保障每个网上银行账号的安全是与每个用户切身利益息息相关的。当前大多数个人网上银行依照身份鉴别的手段不同来区分不同的网上银行操作权限。一般认为使用多因素认证方式的个人网上银行称为“专业版”，具有转账、交易等权限；而仅使用传统的用户名密码认证方式的个人网上银行称为“大众版”，只具有信息查询等权限。

研究显示：登录过程中进行多因素认证的个人网上银行已经基本普及，约占 82%，采用 USBKEY 证书认证的方式最为常见达到 79%。（见图 D.1.2、图 D.1.3）

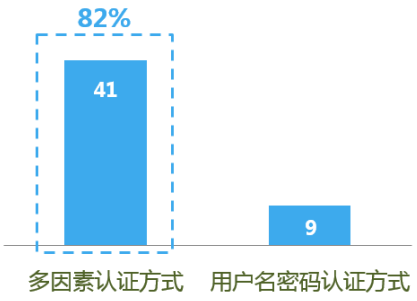
同时，银行依然愿意采用传统的用户名密码认证，并且不仅仅只能通过卡号登录、而是允许用户自定义便于记忆的个性登录名或昵称（见图 D.1.4），但对登录名或昵称长度、密码长度、密码复杂度都有严格的安全策略要求。（见图 D.1.5、图 D.1.6）

“多因素的身份鉴别方式是网上银行登录的关键防线。一个好的身份鉴别方式不但能简化繁杂的登录过程，更能很好地保障用户的账号、财产安全。”

——绿盟科技 工程师 李哲祎

D.1.2 身份鉴别的两种常见方式

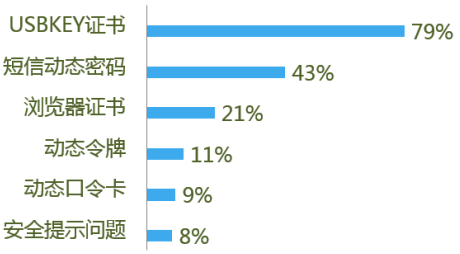
多因素的身份鉴别比传统用户名密码方式更普及



备注：数据样本为中国50大银行。
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

D.1.3 多种多因素认证方式的使用情况比较

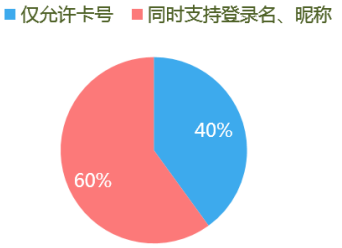
采用USBKEY证书的多因素认证登录方式最为常见



备注：由于各银行个人网银并非支持一种认证方式，因此各种认证方式百分比之和并非百分之百。
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

D.1.4 用户名密码认证方式的使用情况比较

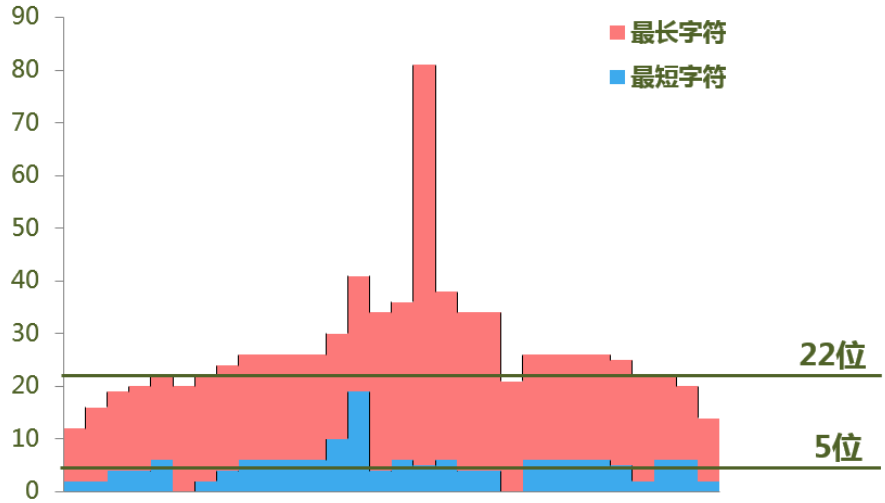
五分之三个人网上银行支持用户自定义登录名、昵称



备注：数据样本为中国50大银行。
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

D.1.5 用户名和密码的安全策略要求更加严格

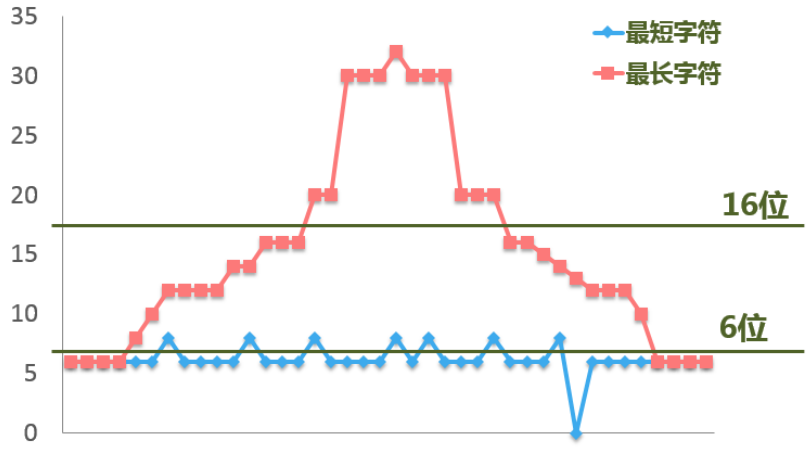
登录用户名长度的正态分布显示其长度策略主要集中在5-22位字符



备注：仅针对研究发现的明确要求用户名长度的30家个人网上银行进行统计

来源：个人网上银行登录安全研究（2013年1月），绿盟科技

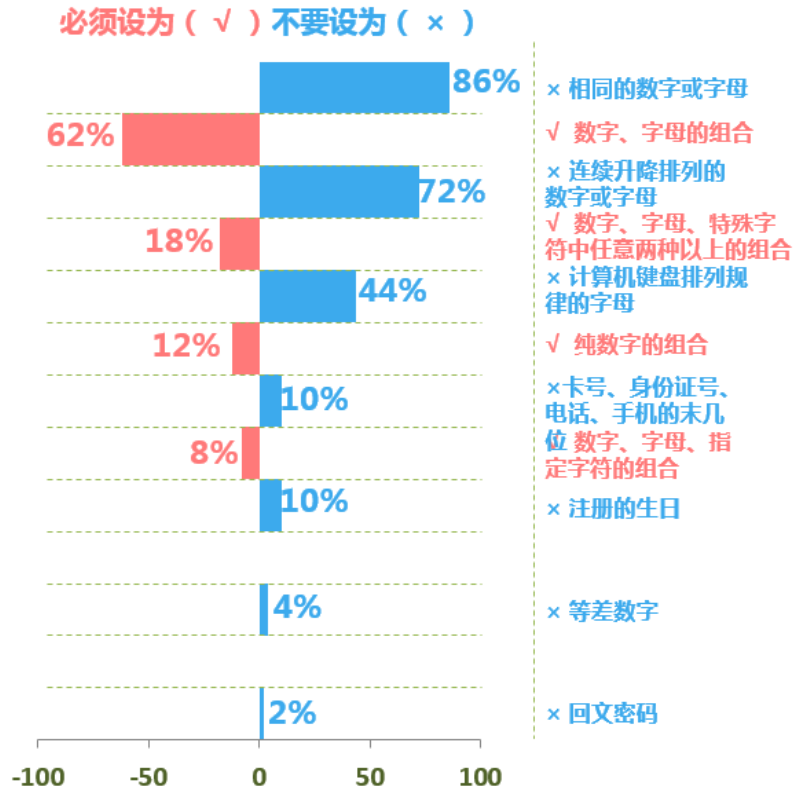
密码长度的正态分布显示其长度策略主要集中在6-16位字符



备注：仅针对研究发现的明确要求密码长度的40家个人网上银行进行统计

来源：个人网上银行登录安全研究（2013年1月），绿盟科技

D.1.6 密码复杂度策略是6-8位短密码实现强鲁棒性的必要保证



备注：1）数据样本为中国50大银行，2）鲁棒是健壮和强壮的意思，
3）回文密码指从左向右或从右向左内容完全相同的密码。

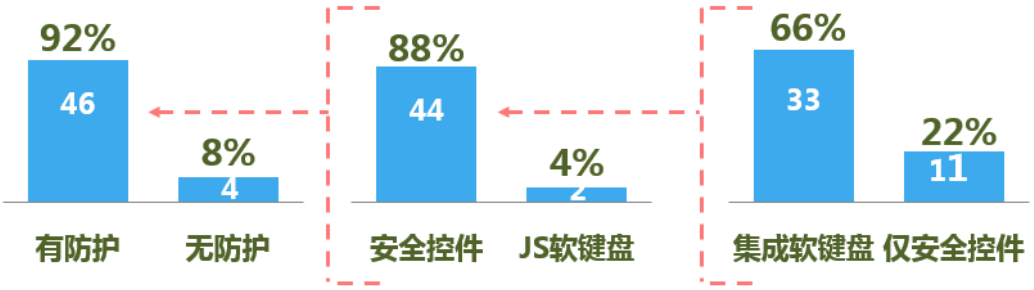
来源：个人网上银行登录安全研究（2013年1月）,绿盟科技

3）对密码的输入保护多采用安全控件集成软键盘的混合模式

登录中的输入安全主要集中于保护卡号、用户名和密码等信息，而密码是保护对象中安全级别要求最高的。当您初次使用个人网上银行时，一般会被提示安装“安全控件”，安全控件即是银行为保障用户输入密码不被木马、病毒、恶意程序等非法获取的最有效的保护措施之一。

研究显示：当前输入保护主要有“安全控件”和“软键盘”两种手段。但当前的部分安全控件已经得到创新，将软键盘的功能集成到控件之中，因此，这种混合模式的安全控件也常被多数网上银行采用。无论采取何种手段保护，86%的密码输入后均会实现自动加密。（见图 D.1.7）

D.1.7 安全控件集成软键盘模式是对密码输入保护的主流方式



备注：JS软键盘是指通过JavaScript技术实现的Web前端软键盘

来源：个人网上银行登录安全研究（2013年1月），绿盟科技

“抗得住逆向、防得住窃听、抵得住溢出的安全控件就应当绽放在网上银行的舞台上！”

——绿盟科技 安全顾问 赵波

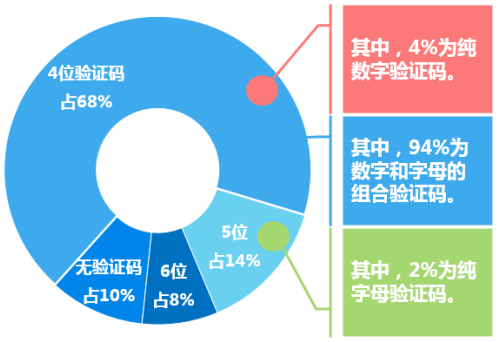
4）验证码依然是登录中不可避免的负面体验

在研究中，我们发现 90%的个人网上银行登录均需要输入验证码，验证码给用户的个人体验依然是负面的——平均延迟用户登录约 2 秒钟。

我们对验证码进行了基础的统计分析：从长度看，多数验证码采用 4 位，也少有采用 5 位或 6 位的情况；从内容看，多数验证码为字母和数字的组合，字母并不区分大小写，也少有为纯数字或纯字母的情况。从展现看，少数银行采用隐藏验证码形式，只有第一次登录失败后，才会显现验证码。（见图 D.1.8）

D.1.8 对登录验证码的认知

4位数字和字母的组合验证码最为常见



备注：数据样本为中国50大银行。

来源：个人网上银行登录安全研究（2013年1月），绿盟科技

5）登录失败策略差异较大，反馈信息多用“友好的错误提示”并模糊化处理

“失败处理”是用户登录个人网上银行失败时，网上银行系统对登录失败采取的安全保护策略，而失败反馈给用户的各种提示信息，被我们称为“错误提示”。常见的错误提示如：账号或用户名错误、密码错误、验证码失效等。

研究显示：登录失败处理的安全保护策略近94%的网上银行采用“账号自动锁定策略”，即达到特定次数的失败登录，账号会自动锁定特定时间，而满足特定时间后，账号再自动解锁。（见图 D.1.9）

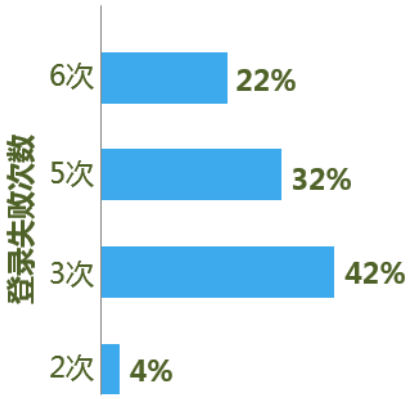
其次，登录失败后反馈的提示信息近 58%的网上银行采用了“友好的错误提示”，即对提示信息进行模糊化处理——不反馈出现登录失败的具体原因及细节，而使用通用提示信息反馈给用户。（见图 D.1.10）

“网银登录失败策略是一把双刃剑，在使用较为严格的‘账号自动锁定策略’后，过于模糊的反馈提示无法提供使用者足够的帮助，降低用户使用舒适度的同时，增加了错误处理成本。”

——绿盟科技 高级顾问 徐特

D.1.9 对登录失败策略的认知

3次登录验证失败即被锁定最常见



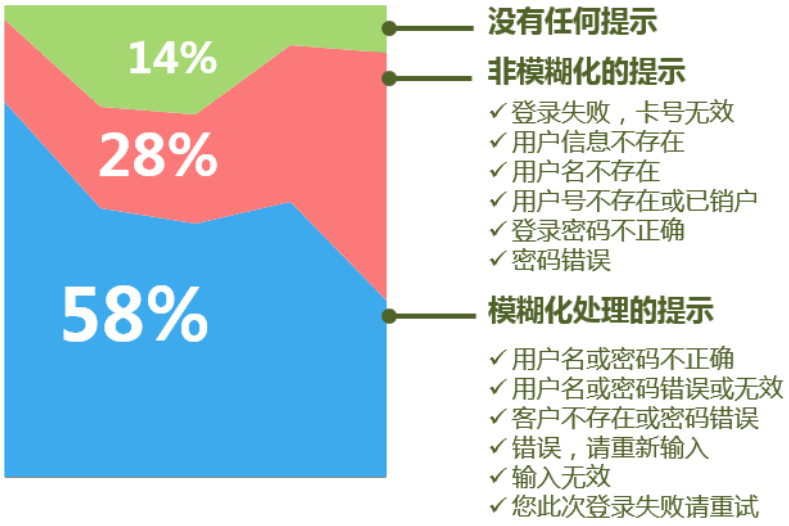
账号自动锁定策略	百分比
锁定，次日自动解锁	40%
锁定，需到柜台解锁	11%
锁定，20分钟后自动解锁	6%
锁定，24小时后自动解锁	6%
锁定，次日自动解锁；累计锁定10次时，需到柜台解锁。	6%
锁定，次日自动解锁；累计15（18）次校验未通过，需到柜台解锁。	6%
锁定，需自助找回，网银重置密码或到柜台解锁。	6%
无自动锁定策略	6%
锁定，5分钟后自动解锁	3%
锁定，30分钟后自动解锁	3%
锁定，2小时后自动解锁	3%
锁定，次日自动解锁，若第二日再次连续4次密码错误，需到柜台解锁。	3%
锁定，需客服电话解锁，或到柜台解锁	3%

备注：数据样本为中国50大银行。

来源：个人网上银行登录安全研究（2013年1月），绿盟科技

D.1.10 对登录失败后错误提示信息的认知

58%的登录失败采用“友好的错误提示”，进行了模糊化处理



备注：数据样本为中国50大银行。

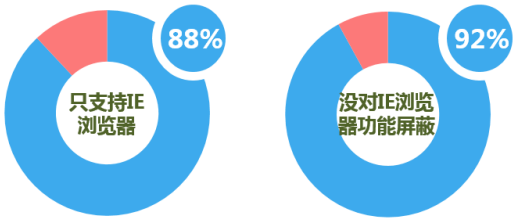
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

6）少数银行对客户端的浏览器要求更精细

“浏览器功能屏蔽”是银行为防范个人网上银行客户端风险，采取的屏蔽客户端浏览器部分功能的措施。一般包括：屏蔽菜单栏功能、屏蔽导航栏功能、屏蔽右键功能等。

值得关注的是，在被研究的 50 大银行中，88%的个人网上银行仅支持客户端使用 IE 浏览器，而在仅支持 IE 浏览器的个人网上银行中，92%没有对 IE 浏览器进行“功能屏蔽”的措施。反之，少数银行支持除 IE 以外两种或更多浏览器，并分别不同程度采用了“功能屏蔽”的安全加强措施。（见图 D.1.11）

D.1.11 多数银行对客户端的浏览器关注不够



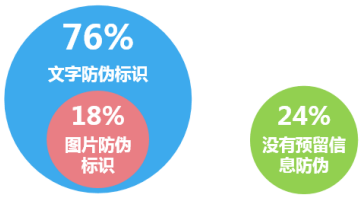
备注：数据样本为中国50大银行。
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

7）预留信息的作用并不明显

预留信息是银行为帮助用户有效识别个人网上银行，防范不法分子利用假银行网站进行网上诈骗的一项安全措施。用户可以在银行预先记录一些特定信息（即“预留信息”），当登录个人网上银行、在购物网站上进行支付或在线签订委托缴费协议时，网页上会自动显示您预留的特定信息，以便验证是否为真实的网上银行。

研究显示：当前个人网上银行采用的预留信息方式主要以文字防伪标识为主，少数银行也提供图片防伪标识的预留信息（见图 D.1.12）。无论哪种方式，用户对预留信息的使用都不是十分清楚。

D.1.12 76%网上银行登录时采用的预留信息是文字标识



备注：数据样本为中国50大银行。
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

“网银需要对用户进行身份认证，同样，用户也需要确认网银站点的真实性。个性的预留信息能够帮助用户快速、有效识别网银站点的真伪，保护用户资产，应该得到广泛推广和使用。”

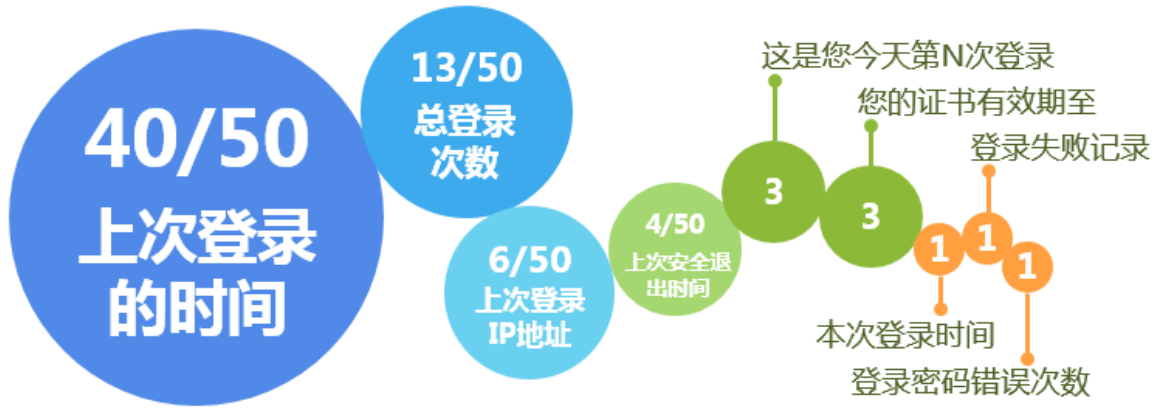
——绿盟科技 项目经理 延晋

8）欢迎首页的登录提醒信息多种多样

当您成功登录个人网上银行后，在其欢迎首页往往提供一些用户个人信息或以往的登录历史信息，我们称其为“登录提醒信息”。这些信息能够方便您了解自己网上银行的使用情况，为您提高网上银行使用的安全意识。

我们的研究显示：当前各网上银行采取的登录提醒信息多种多样，较为多见的是提醒“上次登录的时间”信息；在提醒时间基础上，也有少数银行提醒更加多样，如“总的登录次数”、“上次登录的 IP 地址”、“上次安全退出时间”、“密码错误次数”等。（见图 D.1.13）

D.1.13 80%的网上银行登录提醒信息是”上次登录时间”



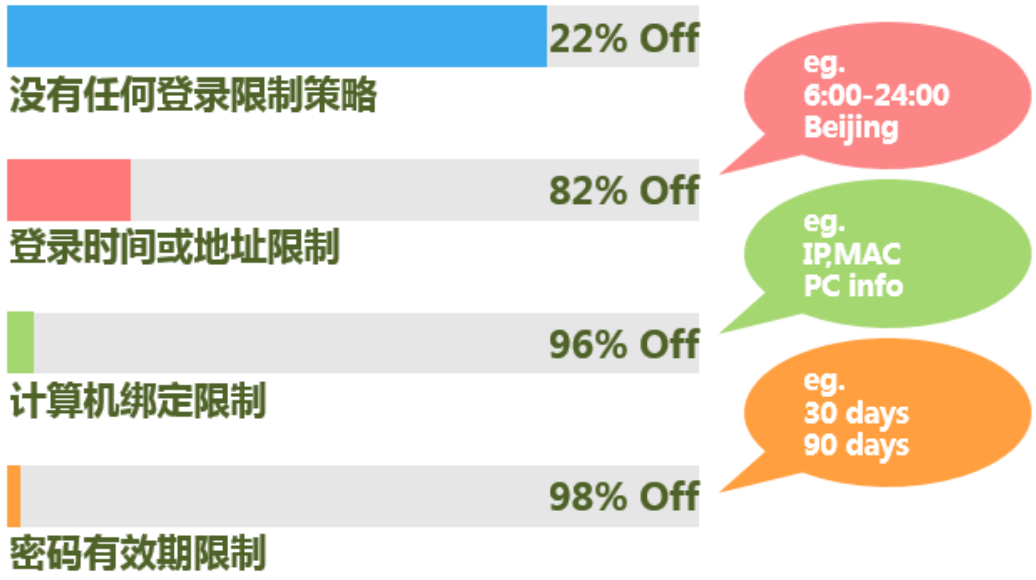
备注：
1）数据样本为中国50大银行。
2）图中N为自然数列。
来源：个人网上银行登录安全研究（2013年1月）,绿盟科技

9）与登录相关的限制策略应用百花齐放、百家争鸣，但效果不佳

在网上银行登录过程中，除登录事件中我们可见的各种安全措施，还有一些非常隐性的措施，以防范各种未知的登录风险，我们称其为“与登录相关的限制策略”，也可理解为“与登录相关的安全加强策略”。

研究显示：限制策略主要体现有四种，分别为“密码有效期限制”、“登录电脑限制”、“登录时间或 IP 地址限制”和“登录频率或地域限制”。只有 11 家银行的个人网上银行具备一项或多项可设置限制策略的功能，但遗憾的是这些功能中多数为被动设置项，而非默认设置项。（见图 D.1.14）

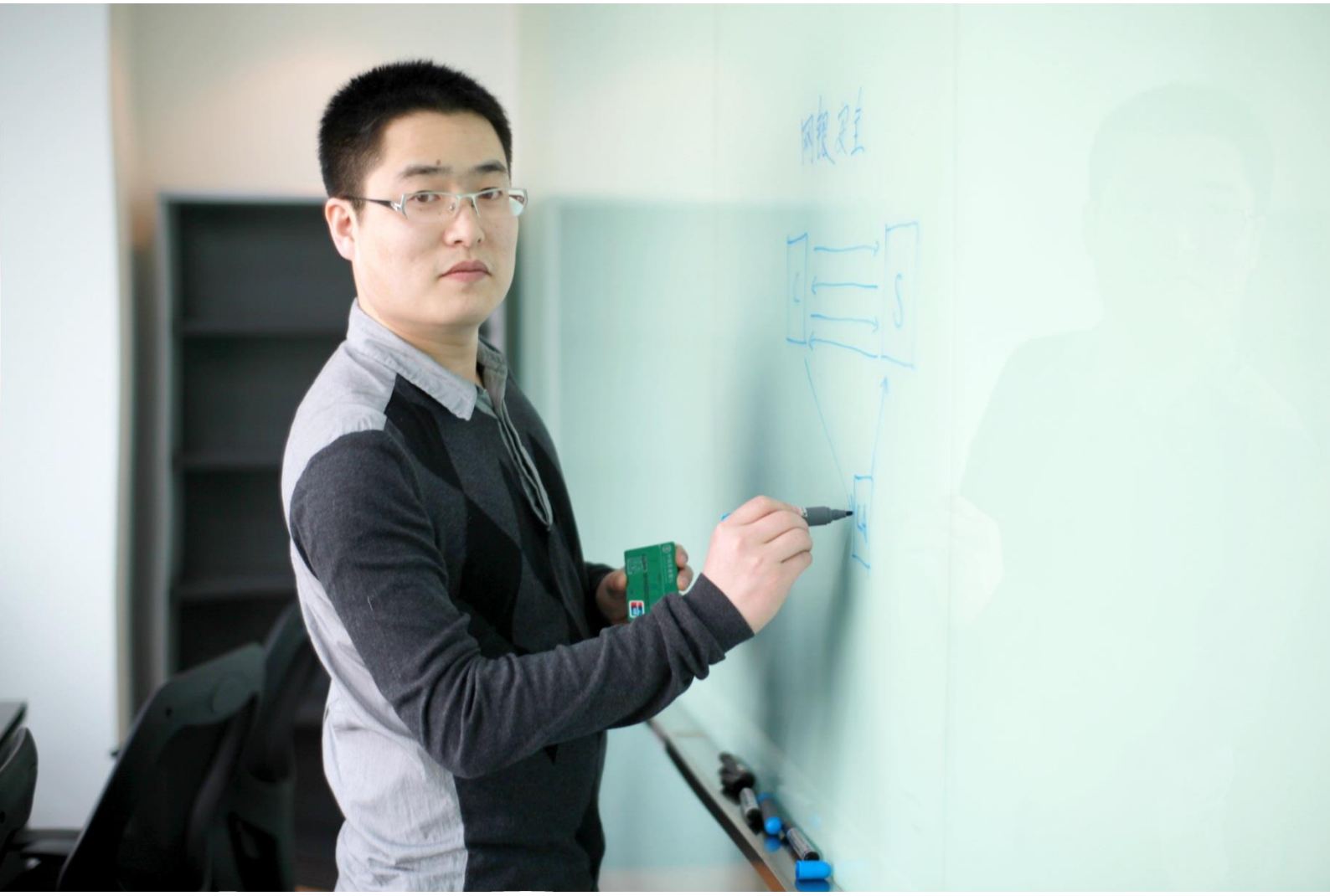
D.1.14 78%的网上银行没有任何登录限制策略



备注：
1）数据样本为中国50大银行。
2）此处Off表示与描述不符的含义。
来源：个人网上银行登录安全研究（2013年1月）,绿盟科技

D2. 攻与防：解决最突出的五大威胁是保障网上银行登录安全的关键

现在，转换您的身份，从一位网上银行用户变成身怀绝技的攻击者或经验丰富的安全专家，来深入洞察我国各银行个人网上银行登录的攻与防、对立与统一的和谐之美。



10） 网络钓鱼是个人网上银行登录最大的安全威胁

网络钓鱼是当前网上银行、第三方支付等网站面临的最为严重的威胁之一。从技术原理上看，网络钓鱼并不高深，但之所以造成的影响很大是因为其本质是利用人的无知或心灵的弱点。（见图D.2.1）

网络钓鱼威胁会直接带来经济损失。从防御角度银行设计了“预留信息”的功能和采用扩展验证(EV)SSL证书进行可信提醒，这些防御措施都有一定的局限性，其效果因用户的安全意识和安全习惯而异。

通过我们的调研与分析认为：银行方面应加强网上银行用户者安全意识的宣贯工作，促使用户养成良好的安全使用习惯，才能更好的发挥网上银行安全措施的作用。

预留信息和可信提醒的方式在合理运行的前提下，才可以发挥较好的防网络钓鱼攻击能力。

D.2.1 网络钓鱼的一般过程示意

来源：《绿盟科技反钓鱼整体解决方案》，绿盟科技

“钓鱼网站的存活期以小时计算，仅靠黑名单的防护方法并不及时和足够，如何在客户端动态有效的甄别钓鱼网站是一项有挑战性的课题。”

——绿盟科技 项目经理 蔡昆

11） 恶意代码攻击与网上银行登录紧密相关

恶意代码攻击从未停止脚步，攻击的技术和手法不断翻新，攻击的战场也慢慢转移到涉及经济利益的网上银行领域。恶意软件与杀毒软件的较量可谓从古至今，在网上银行这个战场上，安全控件成为恶意软件新的对手。安全控件使尽全身解数保护用户输入的敏感数据，恶意软件则绞尽脑汁从不同的深度截获敏感信息，这种对抗从Windows消息、键盘驱动与中断、应用层API函数等方面再到内核设备过滤技术方面都一直进行着。因此，安全控件防窃听能力的优劣需要进行深入全面的测试。另外，攻击者对安全控件的鲁棒性程度也觊觎已久，通过逆向分析和模糊测试的方法不断地冲击着安全控件的防御壁垒。

61%

安全控件能够防御

常见的

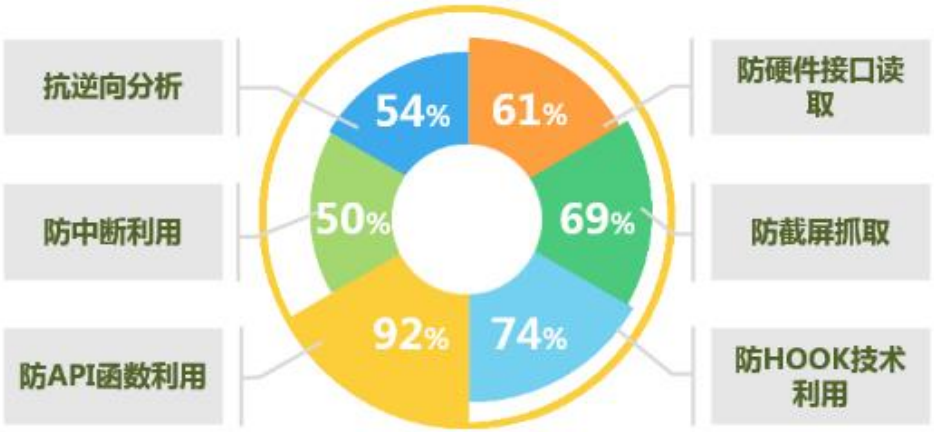
恶意代码截获

攻击

通过我们的调研与分析发现：在采用安全控件的网上银行中，多数安全控件能够防御常见的截获攻击，如Windows API截获、HOOK截获、键盘中断等，并且近半数的安全控件具备抗逆向分析的能力。另外，在使用软键盘的网上银行中，近半数软键盘进行了防截屏设计。（见图D.2.2）

针对恶意代码攻击的防范，当前大多采用了安全控件技术，但安全控件对抗恶意代码和逆向分析的能力还有一定的提升空间。

D.2.2 防API函数利用技术效果较好，防中断和抗逆向能力有待提升



备注：
1）数据样本为中国50大银行。
2）百分数采取四舍五入取整。
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

12） 暴力破解攻击在逐步降低，但仍不可忽视

暴力破解攻击一度风靡，利用自动化的软件，可获得大量使用较弱口令的登录账户，验证码技术应育而生，具备抗OCR（Optical Character Recognition，光学字符识别）能力的验证码技术极大地削弱了自动化暴力破解。网上银行在进行登录暴力破解防御方面主要采用限制策略和验证码技术两类安全措施。针对指定账户的暴力破解是采用限制策略方式防范——超过允许的密码错误次数后，进入锁定状态。各家银行锁定状态持续时间不同，多数为次日自动解锁，也有少数银行需要本人持有效证件到柜台办理。一旦账户锁定对于急于使用网上银行的用户来说，次日自动解锁的时限也是无法接受的。限制策略解决了“针对指定账户的暴力破解”，验证码主要是防范“同一弱口令，不同登录账号”的猜测攻击。

通过我们的调研与分析认为：由于限制策略和验证码的使用，使暴力破解攻击成功率大大降低，在成本远大于利益的现实面前，暴力破解攻击事件正在逐步降低。同时，由于用户的安全意识薄弱，少数银行对密码的要求不是十分严格，也造成了暴力破解攻击一直持续不断，仍不可忽视。我们相信：随着网上银行限制策略的不断丰富、具备抗OCR能力的验证码不断完善，将会大大地削弱暴力破解攻击，使网上银行防护效果更好。

13） 登录中的恶意滥用问题尚无非常有效的解决办法

恶意滥用攻击多发生在USBKEY不参与登录的情况下，攻击者针对获得的银行卡号或登录昵称刻意多次输入错误密码，导致被攻击的用户账号锁定。少数银行针对此类锁定需要用户本人携带有效证件到柜台办理解锁操作，给用户带来不便的同时，也会影响到银行的工作效率和信誉。

目前银行针对此类恶意滥用的攻击采取的是验证码技术，避免攻击者通过自动化的工具实现大范围批量的账户锁定，但还是无法避免有针对性的恶意锁定账号攻击。

通过我们的调研与分析认为：采用验证码功能削弱自动化的大范围批量恶意滥用的程度与验证码自身的强度成正比。目前验证多为4位数字和字母的组合，抵抗OCR的能力欠缺。

目前对于有针对性的恶意的账号锁定攻击尚无较有效的防护措施。

14） 用户身份假冒是当前登录面临的最头痛问题

在用户身份假冒攻击中，攻击者与受害者有两种简单的关系：熟知和不知。熟知关系的攻击者可以轻易的盗取受害者的登录凭证（如：卡号、密码、USBKEY等），从而假冒受害者身份进行网上银行操作；不知关系的攻击者要进行攻击需要一定的攻击场景，如：处于同一个局域网环境，包括办公局域网、公共WIFI网络等，攻击者利用ARP或代理拦截等技术攻击获取用户登录凭证，假冒受害者身份进行网上银行操作。

目前银行针对身份假冒攻击的防护，从登录过程和登录反馈两个方面进行防护。其一是采用HTTPS协议利用数字证书进行身份验证，对“中间人攻击”进行提示并结合安全控件技术对敏感数据进行加密，即便陷入中间人攻击，也无法破译登录凭证；其二是利用登录成功短信提醒和显示上次登录信息（包括：登录时间、登录IP地址、登录失败次数等）方式及时提醒用户可能存在的假冒登录。

通过我们的调研与分析认为：采用HTTPS结合USBKEY数字证书技术，严格遵守SSL过程进行双向身份鉴别的防护效果较好，基本杜绝中间人攻击。此类防护中USBKEY鲁棒性是防御的重中之重。短信提醒和上次登录信息的功能起到缩短发现时间，及时采取应对措施的作用。但还需要银行方面加大安全措施的宣传力度，网上银行用户提高安全防范意识，同时默认启用或开通相关的安全功能。

目前网上银行通常会提供两种版本的登录——大众版和专业版。大众版采用HTTPS通信结合安全控件方式，无法避免中间人攻击，但通过安全控件可保护登录凭证，控件的加密强度和抗逆向分析能力成为攻防焦点；专业版采用HTTPS通信、安全控件以及USBKEY方式。但大多数USBKEY在登录环节并未使用，使得登录防护效果与大众版相同。另外，登录提醒和提示信息量还有待丰富，以便网上银行用户能更清晰地进行危险判断。

安全控件成为攻防焦点，USBKEY充分利用成为趋势，用户安全意识提升仍需继续。

“对银行来说，网上银行不仅是一个产品，更应是一件艺术品；对用户来说，大众最受欢迎的艺术品，就是大家最佳的投资选择。”

——绿盟科技 高级顾问 刘凯

D3.监管：合规不是终点而是起点，不要输在起跑线

现在，转换您的身份，从一位网上银行攻击者或安全专家再次变成银行业监管机构的安全监察人员，随同我们一同探索个人网上银行登录中的安全合规要求符合情况。

目前较为详细、可参考价值最高的网上银行合规要求是由中国人民银行于 2012 年 5 月 8 日发布的《网上银行系统信息安全通用规范》（以下简称《通用规范》）。该规范涉及网上银行系统的技术、管理和业务运作三个方面，分为基本要求和增强要求两个层次，基本要求为对网上银行系统的最低安全要求，增强要求为三年内应该达到的安全要求。依此规范，我们将登录相关的主要安全内容从三方面展开讨论，即：网络通信、安全控件和软键盘，以及图形验证码。

15） 加密通信协议已经普及，弱加密算法尚存

对于数据传输过程来说，最重要的就是数据信道的安全。防窃听、防劫持刻不容缓。要解决该问题，就取决于传输协议的安全性以及加密算法的强壮程度。

以上两项内容在《通用规范》通讯协议相关条目中有明确地要求：

- 应使用强壮的加密算法和安全协议保护客户端与服务器之间所有连接，保证传输数据的机密性和完整性，例如，使用 SSL/ TLS、IPSEC 和 WTLS 协议。
- 如果使用 SSL 协议，应使用 3.0 及以上相对高版本的协议，取消对低版本协议的支持。

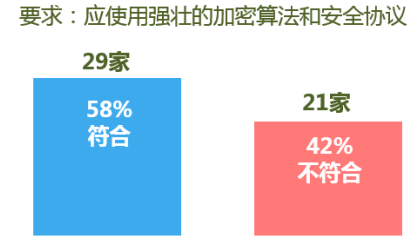
我们在对网上银行支持的加密算法进行安全合规性分析后发现，有多家银行不同程度地提供了对 SSL 弱加密算法的支持。支持的 SSL 弱加密算法主要包括如下：

TLS_RSA_WITH_DES_CBC_SHA
TLS_RSA_EXPORT1024_WITH_RC4_56_MD5
TLS_RSA_EXPORT1024_WITH_RC4_56_SHA
TLS_RSA_EXPORT1024_WITH_DES_CBC_SHA
TLS_RSA_EXPORT_WITH_RC4_40_MD5
TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5

若在传输中使用了弱加密算法，将使数据传输的安全性大大降低。（见图 D.3.1）

另外，在研究对象中，无一例外地均使用了 SSL 3.0 或 TLS 1.0 协议作为其网上银行加密传输协议，并且均不支持存在安全问题的低版本的 SSL 协议，因此该项合规达标率达到了 100%。

D.3.1 近半数网上银行HTTPS应用实现方式不符合合规要求



备注：
1）数据样本为中国50大银行。
2）百分数采取四舍五入取整。
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

“事实证明没有绝对安全的加密算法，各行加密算法的选择主要取决于加密速度、资源消耗以及安全性要求等几个关键因素的综合考虑。在传输客户认证信息的网银登录阶段，应尽量选择强度较高的加密算法以最大程度的规避用户信息泄密风险。”

——绿盟科技 高级顾问 齐芳

16） 安全控件和软键盘广泛使用，但技术细粒度有待加强

在这个病毒、木马泛滥的年代，多种网上银行盗号程序在互联网中广泛传播。为了防止恶意程序盗取用户的网上银行账号、密码等敏感信息，各家银行都不同程度上采用了多种技术手段来保障用户的网上银行安全。

由“D1.现状”中图 D.1.7 可知，大部分银行采用了安全控件或软键盘的方式来进行输入保护，而采用安全控件集成软键盘功能的混合方式成为了网上银行安全输入保护的新趋势。值得一提的是，有 8%的银行未采取任何有效措施来保护用户的输入信息，一旦用户的终端遭受网上银行盗号程序的攻击，用户账号、密码等隐私将直接暴露给攻击者。

针对网上银行控件及软键盘的安全防护方式，《通用规范》提出了如下具体要求：

基础要求：

- 客户端程序应具有抗逆向分析、抗反汇编等安全性防护措施，防范攻击者对客户端程序的调试、分析和篡改。
- 客户端程序应防范恶意程序获取或篡改敏感信息，例如使用浏览器接口保护控件进行防范。
- 客户端程序应防范键盘窃听敏感信息，例如防范采用挂钩 Windows 键盘消息等方式进行键盘窃听，并应具有对通过挂钩窃听键盘信息进行预警的功能。

增强要求：

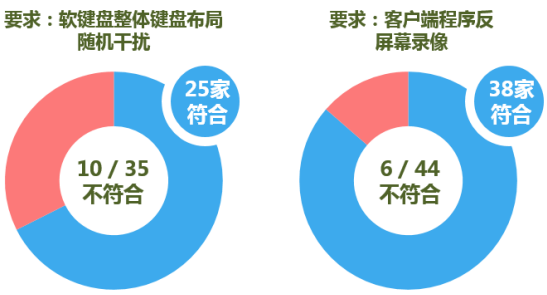
- 客户端程序应保护在客户端启动的用于访问网上银行的进程，防止非法程序获取该进程的访问权限。
- 客户端程序应采用反屏幕录像技术，防范非法程序获取敏感信息。
- 使用软键盘方式输入密码时，应采取对整体键盘布局进行随机干扰等方式，防范密码被窃取。

在安全防护中使用最广泛的安全控件方面，部分控件不具有抗逆向分析能力，攻击者很可能通过调试、篡改等方式绕过部分安全控件的防护手段，造成安全控件的失效。

网上银行安全控件的最主要功能就是使用多种手段防范挂钩行为的攻击，但是由于控件本身技术实现原理的不同，有些无法防范驱动级别及操作系统内核级别的键盘钩子。

在软键盘防护技术方面，部分银行未按照《通用规范》要求对键盘布局进行随机干扰或排序，有些银行只对数字键盘部分进行了随机排序但随机性不强——恶意木马程序可能通过记录鼠标的坐标轨迹，然后结合软键盘的位置猜测出用户输入的密码信息。多数单纯使用软键盘方式的银行未能防范屏幕录像技术，因此也为攻击者直接获取到用户账号、密码带来了可能。（见图 D.3.2）

D.3.2 大多数网上银行软键盘或安全控件符合合规要求



备注：数据样本为中国50大银行。
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

“信息安全的实践告诉我们一个事实，没有100%的安全，网上银行的安全也同样如此，因此建议各网上银行应当努力提高网银自身的抗打击能力，最大限度地提高攻击的成本和实施攻击的难度。对网银客户端安全应当综合采取防护、管理、控制、审核等多层次、协调一致的安全措施。”

——绿盟科技 资深顾问 白雷

17） 图形验证码安全合规性不容乐观

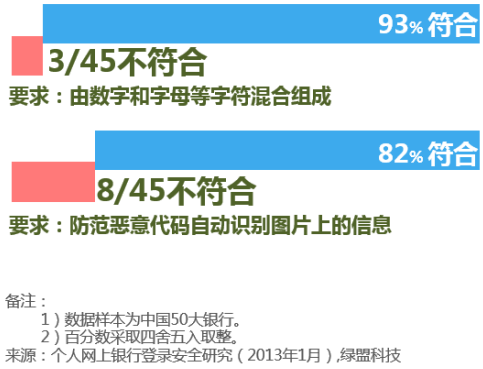
当前，图形验证码是最好的识别网上银行用户正常登录行为与大规模恶意自动化登录脚本攻击最好的方式。它在防止账号被暴力破解攻击方面起到了十分重要的作用。《通用规范》中，对图形验证码提出了详细具体的要求：

应具有防范暴力破解静态密码的保护措施，例如在登录和交易时使用图形认证码，图形认证码应满足：

- 由数字和字母等字符混合组成
- 随机产生
- 采取图片底纹干扰、颜色变换、设置非连续性及旋转图片字体、变异字体显示样式等有效方式，防范恶意代码自动识别图片上的信息
- 具有使用时间限制并仅能使用一次
- 图形认证码应由服务器生成，客户端源文件中不应包含图形验证码文本内容

我们对验证码合规性检查和分析发现：在验证码使用方面，有 45 家银行在登录过程中使用了图形验证码，另外两家银行使用了在 URL 中携带 Token 的方式来防范自动化的攻击行为。值得注意的是，在使用了验证码的银行中，有一定数量的银行在用户打开网上银行登录页面首次登录时并不要求输入图形验证码，只有登录失败后，才需要输入图形验证码进行识别——这一设计方便了用户使用，提高了用户体验，很好地达到了网上银行登录易用性与安全性的平衡点。

D.3.3 少数网上银行验证码不符合合规要求



备注：
1）数据样本为中国50大银行。
2）百分数采取四舍五入取整。
来源：个人网上银行登录安全研究（2013年1月），绿盟科技

在图形验证码设计方面，验证码内容构成和抗 OCR 能力都有少数银行不符合合规要求。（见图 D.3.3）除了验证码图片本身的设计方面外，有部分网上银行系统在验证码功能实现方面，也都存在不同程度的问题。如：验证码有效期、更新机制实现错误，在用户输入错误后验证码未能及时刷新，造成验证码可以重复使用，有些银行的验证码在被正确验证并使用后，并未作失效处理，使其仍可以被用于登录尝试，造成了验证码的重复使用缺陷。

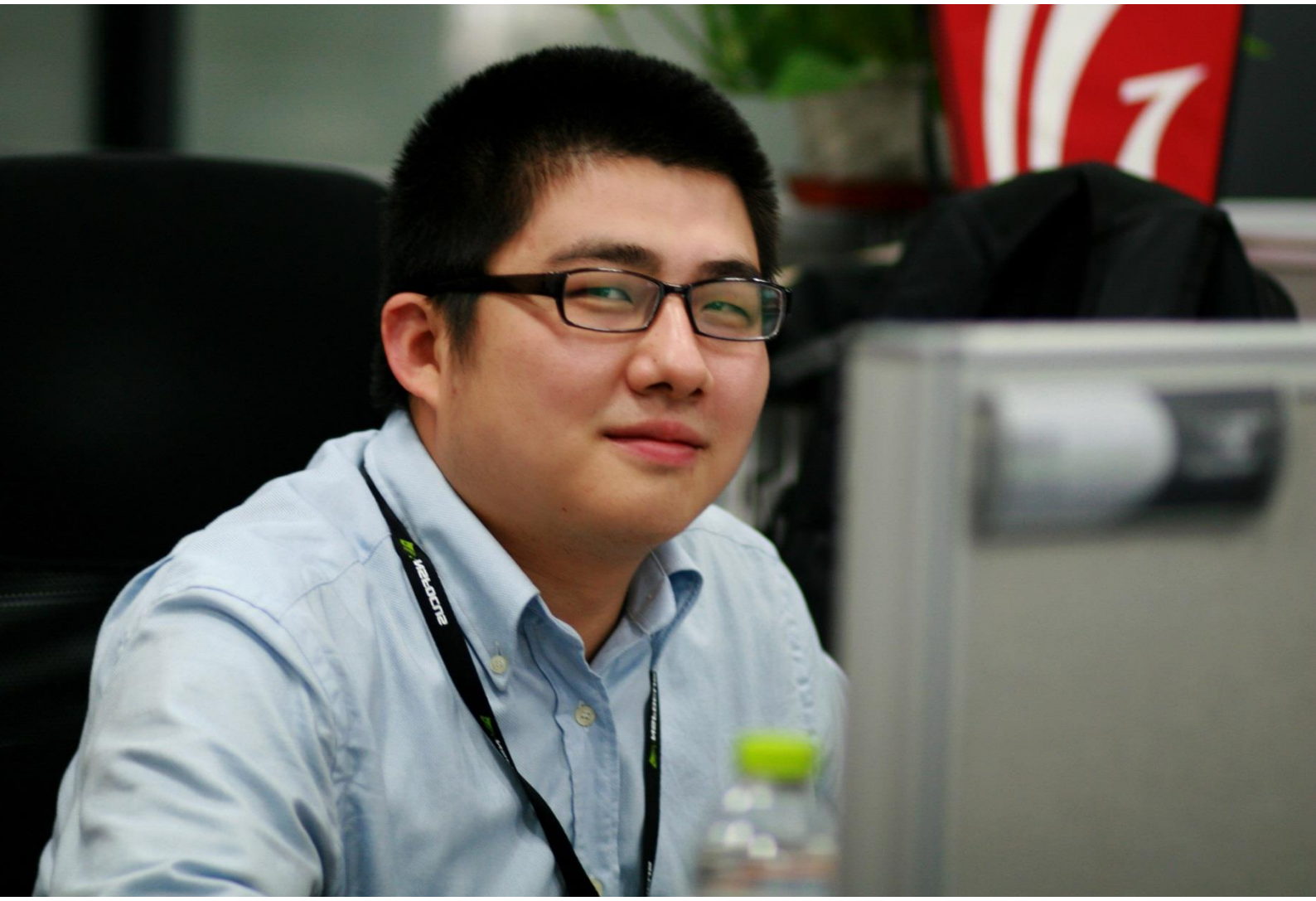
“虽然图形验证码可以有效防止自动化工具的批量猜测，但应对人工打码方式的猜测还是力不从心，还应结合多种安全策略如登录地域、IP 地址、时间、次数等限制策略综合防护。”

——绿盟科技 安全顾问 陆辉

D4.局限性：技术也有不足，得与失都得自己承担

现在，转换您的身份，从一位网上银行安全的监管者最后变成架构设计或开发的技术人员，来和我们一同客观、准确的探讨一下个人网上银行登录中的主要安全措施技术的优与劣。

本报告中提到的“九类”个人网上银行安全防护措施中，我们根据技术与实现的普遍性，选取身份鉴别、输入保护、验证码这三类主要技术应用进行分析和探讨。



18） 利用 USBKEY 证书的登录身份鉴别，也有硬伤

当前网上银行的USBKEY硬件主要针对证书安全的存放、数据的加密、身份的认证等方面进行应用，使用 USBKEY 硬件能够避免当传统的用户名、静态密码被盗取而造成的损失，大大提高了网上银行使用的安全性。

USBKEY 作为独立的硬件设备，其主要体现了下面几处优点：

1） 黑客需要同时取得用户的 USBKEY 硬件以及用户的 PIN 码，才可以登录系统。即使用户的 PIN 码被泄漏，只要用户持有的 USBKEY 不被盗取，合法用户的身份就不会被仿冒；如果用户的 USBKEY 遗失，拾到者由于不知道用户 PIN 码，也无法仿冒合法用户的身份。

2） USBKEY 使密钥存储于安全的介质之中，外部用户无法直接读取，对密钥文件的读写和修改都必须由 USBKEY 内的程序调用。从 USBKEY 接口的外面，没有任何一条命令能够对密钥区的内容进行读出、修改、更新和删除，很好的保证了存储介质的安全性。

3） 公钥密码体制和数字证书从密码学的角度上保证了 USBKEY 的安全性，在 USBKEY 初始化的时候，先将密码算法程序烧制在 ROM 中，然后通过产生公私密钥对的程序生成一对公私密钥，公私密钥产生后，公钥可以导出到 USBKEY 外，而私钥则存储于密钥区，不允许外部访问。进行数字签名时以及非对称解密运算时，有私钥参与的密码运算只在芯片内部即可完成，全过程中私钥可以不出 USBKEY 介质，以此来保证以 USBKEY 为存储介质的数字证书认证在安全上无懈可击。

4） USBKEY 内置 CPU 或智能卡芯片，可以实现数据摘要、数据加解密和签名的各种算法，加解密运算在 USBKEY 内进行，保证了用户密钥不会出现在计算机内存中。

但是，USBKEY 同样存在其缺点，例如：

1） 多数USBKEY的PIN码都是从电脑上输入的，由此攻击者可以通过木马程序直接拦截到USBKEY的PIN码，这也是目前大多数USBKEY存在的一个弱点。知道了 PIN 码后，如果用户忘记将 USBKEY 从电脑上取出，那么攻击者还可以进一步通过PIN码来操作USBKEY。一个非常极端的情况，当个人用户的电脑已经完全被攻击者远程控制，并且所有键盘和屏幕的操作都会被拦截的时候，目前的 USBKEY 是否还能保证安全交易呢？因为此时 USBKEY 的 PIN 码已经完全可能会被黑客拦截，当用户操作完一次 USBKEY 后，假如没有立即拔出 USBKEY，那么攻击者完全可能在这个间歇期伪造一次交易，而此时 USBKEY 以及 PIN 码都可以验证通过。

2） USBKEY 的密钥从“理论”上讲是无法从外部直接读取的，这个“理论”上指的是设计上要绝对安全，如果设计和编写 USBKEY 操作系统 COS（Card Operating System，卡片操作系统）的人在 COS 上留了后门，那么这个人就可以从外部读取 KEY 内部的密钥。

3） 公钥密码体制的确是很安全的，通过复杂的证书管理体系来增加破解的难度，但是数字证书是否是第三方 CA 机构发放的值得深思，并且，当第三方 CA 机构发生安全事故时，如何保证证书的安全？这就让 PKI 安全认证大打折扣了。

4） 虽然 USBKEY 硬件内置 CPU 或智能卡芯片可以完成加密运算，但是数据从电脑上传入 USBKEY 的过程中还是有可能被拦截和修改，USBKEY 内置的 CPU 只能保证自身的运算安全，却难以保证数据传入前不被修改。

“‘没有绝对的安全’同样适用于 USBKEY 身份鉴别。目前第一代 USBKEY 已基本普及，因成本、推广、环保等诸多原因，第二代、三代交互式 USBKEY 还在继续发展中。无论采取何种手段，其本质都是保障用户财产安全，这都是银行义不容辞的责任。”

——绿盟科技 工程师 李哲祎

19） 安全控件是攻与防博弈的矛盾体

为了防止木马在用户输入帐号、密码过程中窃取这些信息，网上银行的安全控件应运而生。当前多数安全控件不仅防止了键盘/消息钩子，而且使通过 IE 的 COM 接口获取密码的方法也无能为力。但是，也有一部分安全控件做得不够底层，技术细节上不够深入，功能还不够完善。

例如，很多安全控件没有考虑对屏幕监控进行限制，常见的有录像，截屏等；也没有对“多键盘输入”或者“远程输入”进行限制，常见的有 USB 键盘，远程桌面登录等。这些无疑会降低安全控件的防范能力，增加用户的风险等级。

从当前“安全控件”与“恶意软件技术”的发展来看，安全控件和病毒、木马等恶意软件有着共同的发展趋势，即拼抢底层驱动，这无疑是一个恶性循环的结果，长此以往，最终受害者将是用户本身。

我们不禁思考：从另一个角度出发，能否建立一种安全控件与恶意软件共存情况下的安全防护解决方案，当然，这些还有待深入研究。

“安全控件也许会成为防病毒厂商的又一得力之作！”

——绿盟科技 安全顾问 赵波

20） 验证码让用户慢下来，影响输入体验

当前 90%的个人网上银行登录采用了验证码，验证码技术成熟，成本低廉，回报率高，能够有效防范软件的自动化操作及暴力破解攻击，是很好的选择。

但是，由于抗 OCR 能力的需要，各种复杂的验证码有时难于辨认，甚至无法正常识别，经常导致用户输入错误，很大程度上影响了用户输入体验和拖长了用户登录时间。

更值得一提的是，当前验证码的实现机制还需要进一步的深化研究，特别是一些缺乏安全思考的开发者错误的实现验证码，将生成图片的信息直接存放于用户 Cookies、URL 中，更有甚者将验证码算法写于 Web 网页中，这些都是不安全、不正确、风险极大的实现。你能正确识别图中的验证码吗？（见图 D.4.1）

D.4.1 少数你能正确识别这些验证码吗？

来源：个人网上银行登录安全研究（2013年1月），绿盟科技

“随着 OCR 技术的加强，变形、拉伸、扭曲等传统对抗手段对使用者越发的不友好，基于逻辑的‘图灵测试’开始取代数字字母验证码，二位数四则运算和中文问答是其中的先行者。”

——绿盟科技 高级顾问 徐特

E. 关于

绿盟科技

北京神州绿盟信息安全科技股份有限公司（以下简称绿盟科技）成立于 2000 年 4 月，总部位于北京。在国内外设有 30 多个分支机构，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。

作者和贡献者

作者：

刘凯	赵波	李哲祎
绿盟科技北京分公司	绿盟科技北京分公司	绿盟科技北京分公司
高级顾问	安全顾问	工程师
Liukai@nsfocus.com	Zhaobo@nsfocus.com	Lizheyi@nsfocus.com

贡献者：

李海涛	项目经理	Lihaitao@nsfocus.com
徐特	高级顾问	Xute@nsfocus.com
延晋	项目经理	Yanjin@nsfocus.com
白雷	资深顾问	Bailei@nsfocus.com
齐芳	高级顾问	Qifang@nsfocus.com
陆辉	安全顾问	Luhui@nsfocus.com
史琛琳	工程师	Shichenlin@nsfocus.com

全球声明

联系我们

北京总部
地址：北京市海淀区北洼路 4 号益泰大厦 3 层
邮编：100089
电话：010-68438880
传真：010-68437328
Email：market@nsfocus.com

更多信息请访问绿盟科技官方网站 http://www.nsfocus.com/

如果您的智能手机上安装了快速条码扫描器，只需扫描此条码，就可直接登录绿盟科技官方网站。

巨 人 背 后 的 专 家

THE EXPERT BEHIND GIANTS