以金融为例，漫谈APT防御

曹岳

国家信息技术安全研究中心

主要内容

一、金融安全态势

二、从几个实例看

三、APT攻防之道

整体安全态势

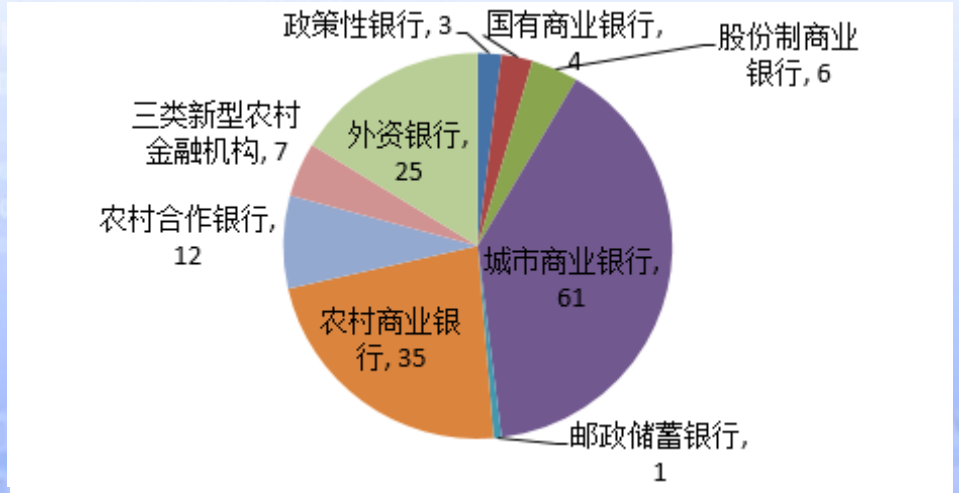
- 从银行抽查情况来看：安全性整体较好
  - 工、农、中、建等24家银行同比安全性较好
  - 认证体系基本完善，技术应用世界领先
  - 系统防护体系趋于成熟，防护能力较高
  - 风险控制体系逐渐形成，安全防护纬度多
  - 政策监管在加强，管理层安全意识强

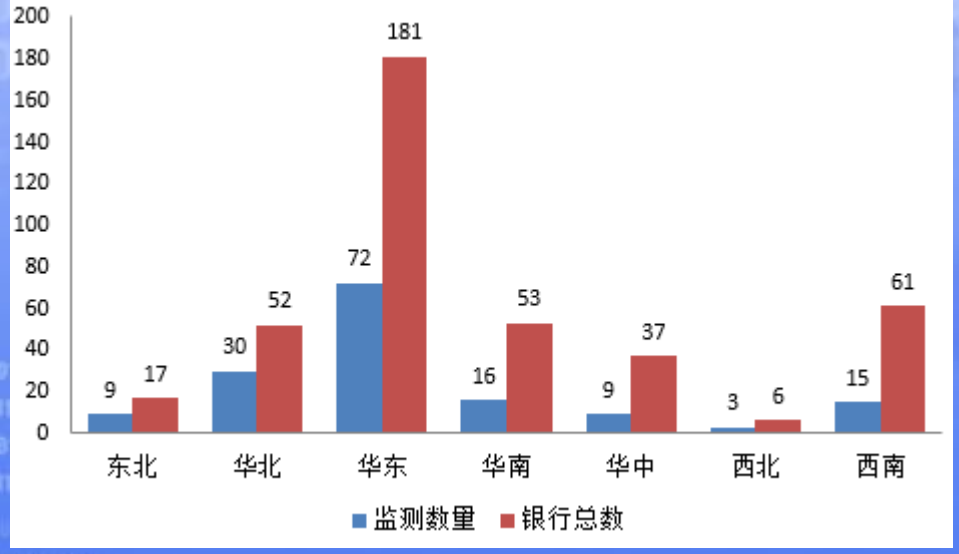
整体安全态势

- 从高强度渗透测试来看：大规模网络攻击风险
  - 远程漏洞监测，20%以上的银行高危
  - 逻辑错误、权限绕过、信息泄漏等业务系统高危漏洞时有发生
- 从国家信息安全战略来看：挑战严峻
  - 国产率较低，自主可控压力较大
  - 系统复杂、防护滞后、安全动态变化、科技风险集中
  - 黑色产业趋利化、集团化、跨境化
  - 相关法律法规、信用体系仍待完善

电子银行漏洞监测

- 安全态势监测对象：

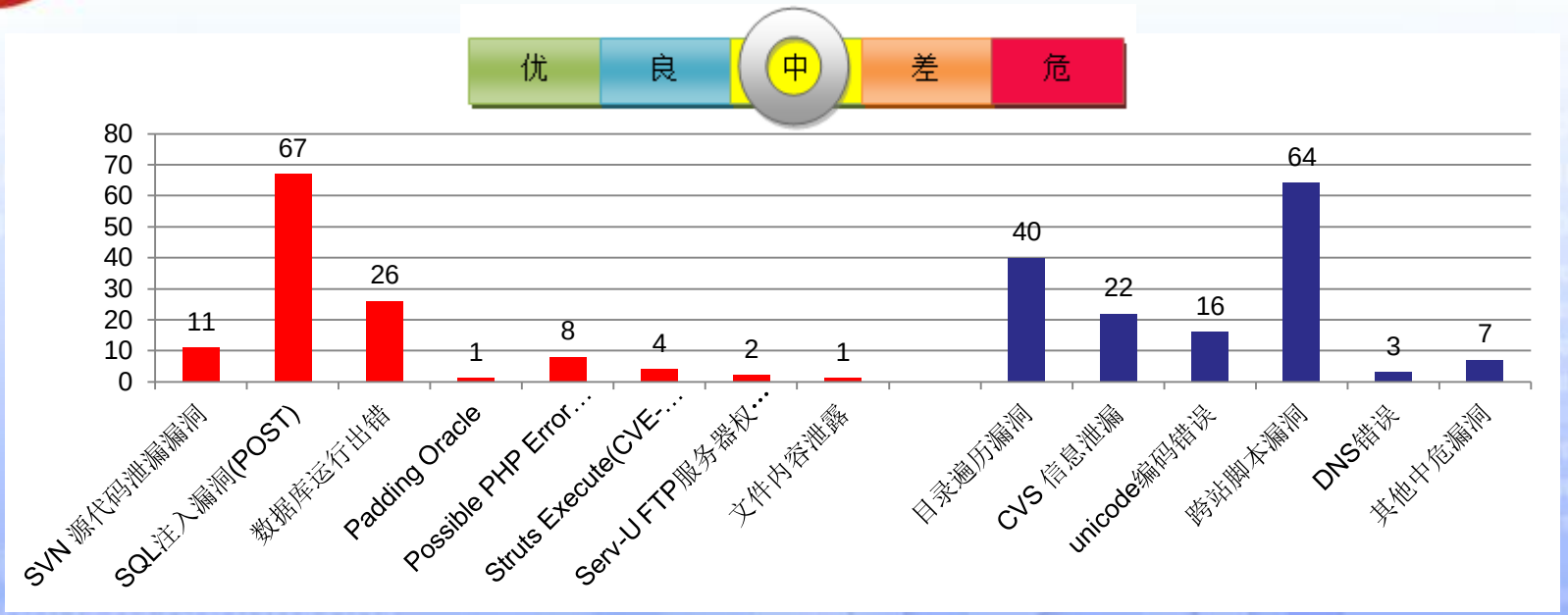




中心抽样检测的对象覆盖全部的七大类银行，包含全部的国有大行、股份制商业银行，部分的城市商业银行、农村商业银行、农村合作银行、三类新型农村金融机构及外资银行。

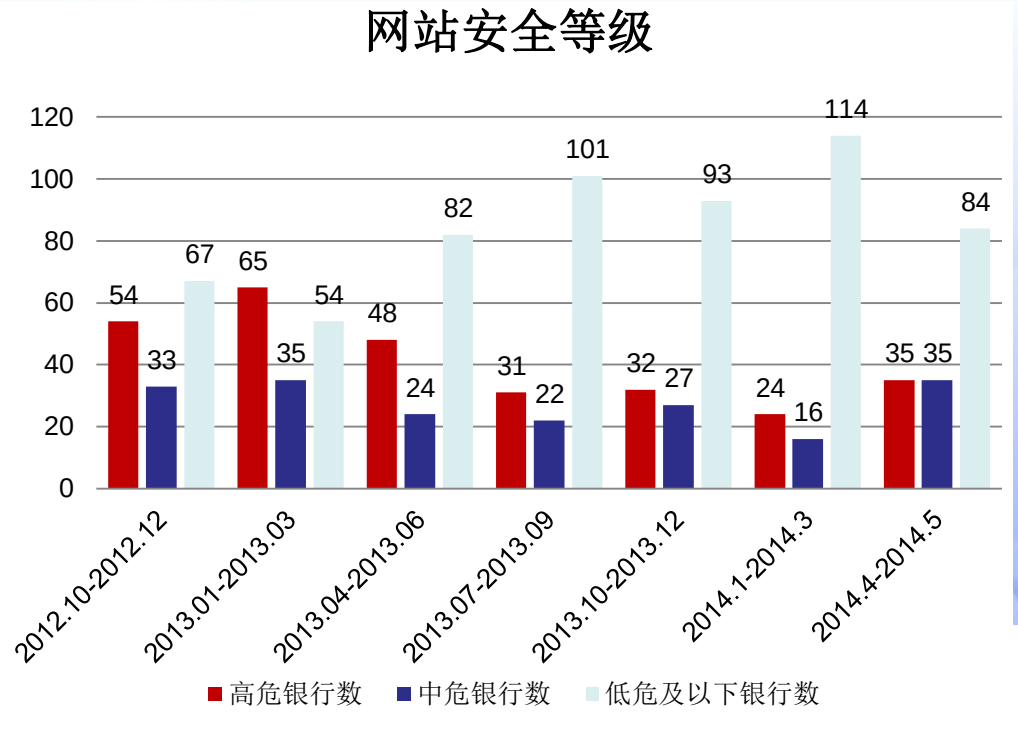
各区域被检测银行数量与银行总数比例大致为1:2（不完全）。

电子银行漏洞监测



- **2014年4月至5月**，国内银行网站安全状况整体评价等级为**中**。主要数据如下：
  - 本次共检测**154家**银行的官方网站，发现**35家存在高危漏洞**，占总数的**23%**；**35**家存在中危漏洞，占比**23%**。
  - 2014年4月至5月存在高危和中危漏洞的银行数量占监测总数比为**45%**，比2014年1月至3月环比上升**19%**。
  - 漏洞攻击手段呈现多样化特点，包括但不限于终端、支付接口、会员系统、邮箱系统、网银伴侣甚至微信公众号银行官方网站、自助等都易成为攻击对象。

电子银行漏洞监测

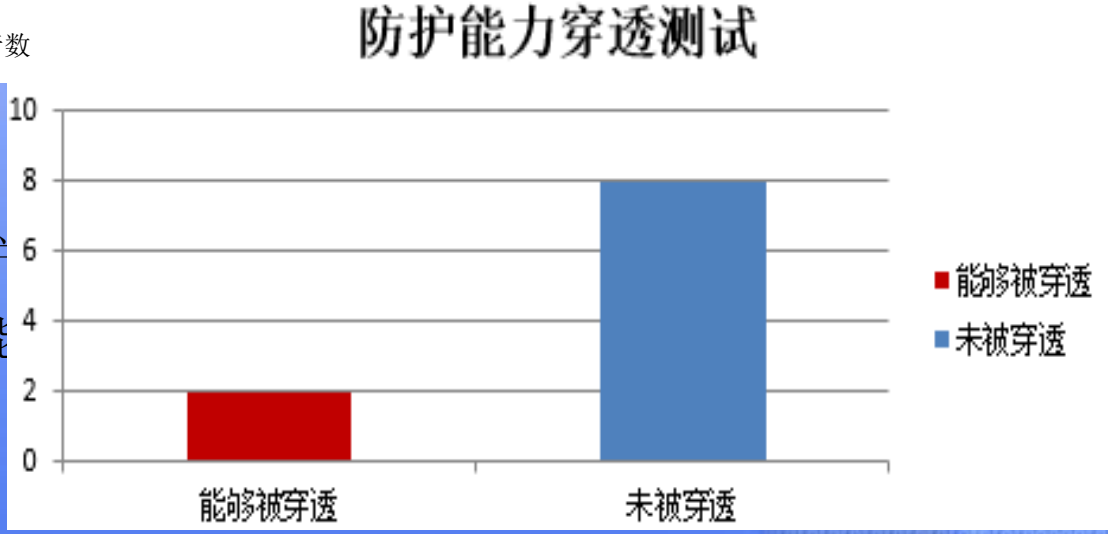


2.漏洞类型统计

本次检测共发现**275个**中、高危漏洞，现阶段威胁银行官方网站安全最主要的漏洞是SQL注入漏洞、数据库运行出错和目录遍历、跨站脚本等漏洞；SVN源代码泄露、PHP报错、CVS信息泄露、unicode编码错误等漏洞也应引起注意。

3.防护能力

中心抽选了10家高危银行进行防护穿透力测试，有**20%**的银行防护能力很低，容易被直接穿透！



电子银行漏洞监测

金融业信息安全风险提示

2013年第2期（总第41期）

中国人民银行办公厅　　签发人：李东荣

根据国家信息技术安全研究中心检测分析，我国部分银行官方网站、网银系统存在安全隐患，现将有关风险提示如下：

一、事件概况

2013年第一季度，国家信息技术安全研究中心通过“国家金融安全检测系统”对一百余家商业银行的官方网站、网银系统进行了监测，发现部分商业银行官方网站存在中危及高危安全漏洞，部分高危安全漏洞可导致银行数据失窃、网站页面篡改、恶意转移客户资金以及业务生产网被进一步入侵等风险，主要安全漏洞包括：

（一）部分银行官方网站系统存在Web漏洞（如钓鱼、SQL注入、挂马等）。

银行网站安全评级比例图

电子银行漏洞监测

监测中危漏洞：跨站脚本攻击

恶意用户可以使用JavaScript、VBScript、ActiveX、HTML语言甚至Flash利用应用的漏洞，从而获取其他用户信息。攻击者能盗取会话cookie、获取账户、模拟其他用户身份，甚至可以修改网页呈现给其他用户的内容。

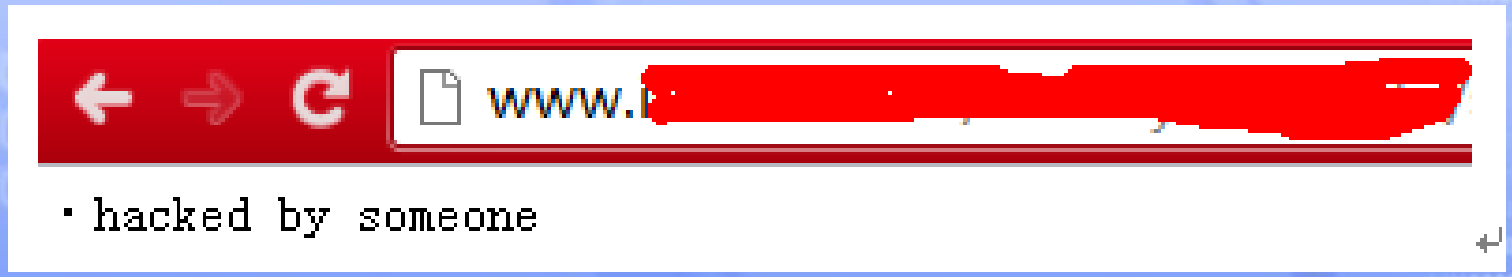
可窃取网银用户的cookie，从而窃取敏感信息。

跨站脚本攻击效果展示

电子银行漏洞监测

监测高危漏洞：SQL注入获取服务器权限

通过此漏洞可以获取数据库权限。利用数据库的管理员权限，可以通过修改数据库的内容修改官方网站的数据，从而实现在主页中显示非法言论、数据获取甚至进一步数据入侵等。如下图所示：



电子银行深度测试

近期，中心对国内20多家网上银行系统进行了深度安全测试，发现不少存在高危漏洞，通过远程渗透，发现通过这些漏洞，能对系统造成非常严重的危害。

主要威胁有：

- 用户资金失窃
- 获取银行机密数据
- 认证机制绕过
- 网站被篡改威胁
- ……

四个经典案例

- 逻辑缺陷
- 信息泄露
- 交易劫持
- 认证绕过

电子银行深度测试

案例一：逻辑缺陷

某银行在帐内转帐过程中可以输入负数，服务器未作验证导致用户**可以远程窃取他人帐号资金。**

不差钱的漏洞

逻辑缺陷漏洞

- 是自动漏洞扫描器很难发现的安全漏洞
- 是攻击者最喜欢利用的安全漏洞之一
- 是使低权限的用户操作高权限的漏洞
- 是可以对系统造成直接损失的安全漏洞

电子银行深度测试

案例二：信息泄露

国内著名网络信息泄露事件

600万用户

CSDN社区 —信息泄露→ 用户名 用户密码 注册邮箱 —危害→ 邮箱被盗 垃圾邮件 账号冻结 丢失账号

工信部 —紧急预案→ 组织专家研讨会 → 加强立法 / 组织安全自查

各大媒体反映强烈

个人对隐私诉求强烈

电子银行深度测试

经过测试发现A银行多处漏洞组合可获取其用户（约8000万）的账号、姓名、身份证号、手机号、存款金额、交易记录等信息

经过测试发现B银行存在安全漏洞，导致数据库833种不同类型的核心数据，包括1.2亿银行账号、银行密码、存款金额等重要数据泄漏。

电子银行深度测试

3亿条银行信息泄漏

金融信息
资金明细
交易记录

可修改信息
账号
密码
手机号

无法修改信息
姓名
身份证号

利用

黑客
掌握的信息比银行还多

隐私机密完全泄露

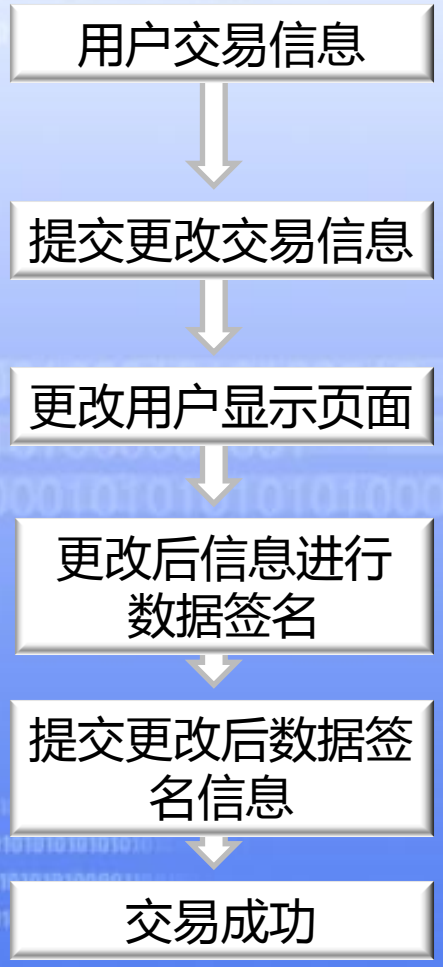
可挽回

无法挽回

银行客户

电子银行深度测试

案例三：UKey交易劫持



在用户不知情的情况下，把钱转到王五的账户上，此类漏洞是一代盾固有的问题。

张三给李四进行转账

提交过程中，卡号户名修改为王五信息

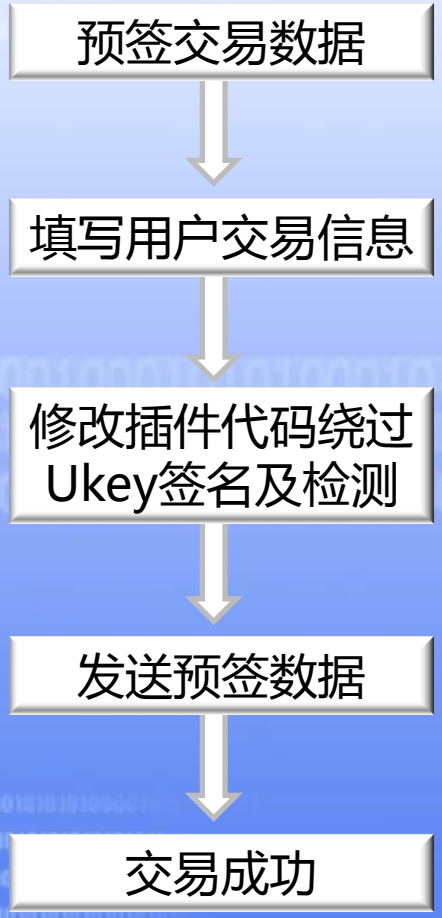
修改服务器返回数据为李四信息，欺骗用户进行下一步操作

修改签名数据为王五信息，进行数据签名

发送王五的数据表单+王五的签名数据

电子银行深度测试

一代Key无盾转账



在无盾的状态下，完整的进行一次转账交易操作，经过分析大多数使用一代Key的城乡行都存在这样的问题

Ukey签名数据无随机数时，预签交易数据

用户正常进行交易信息操作

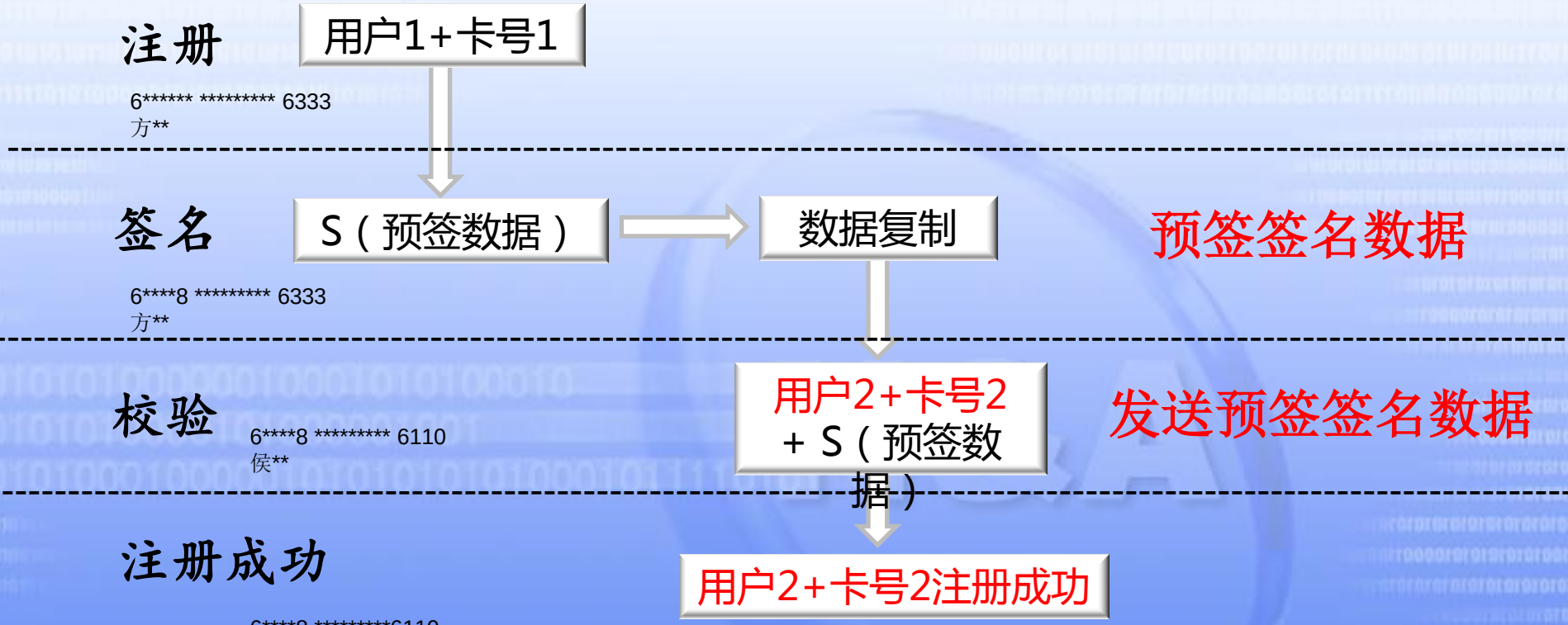
修改ActiveX控件签名数据的代码及其检测Ukey状态的代码，绕过保护

提交此次交易信息+预签数据

在无盾状态下，完整的进行了一次转账交易操作。

电子银行深度测试

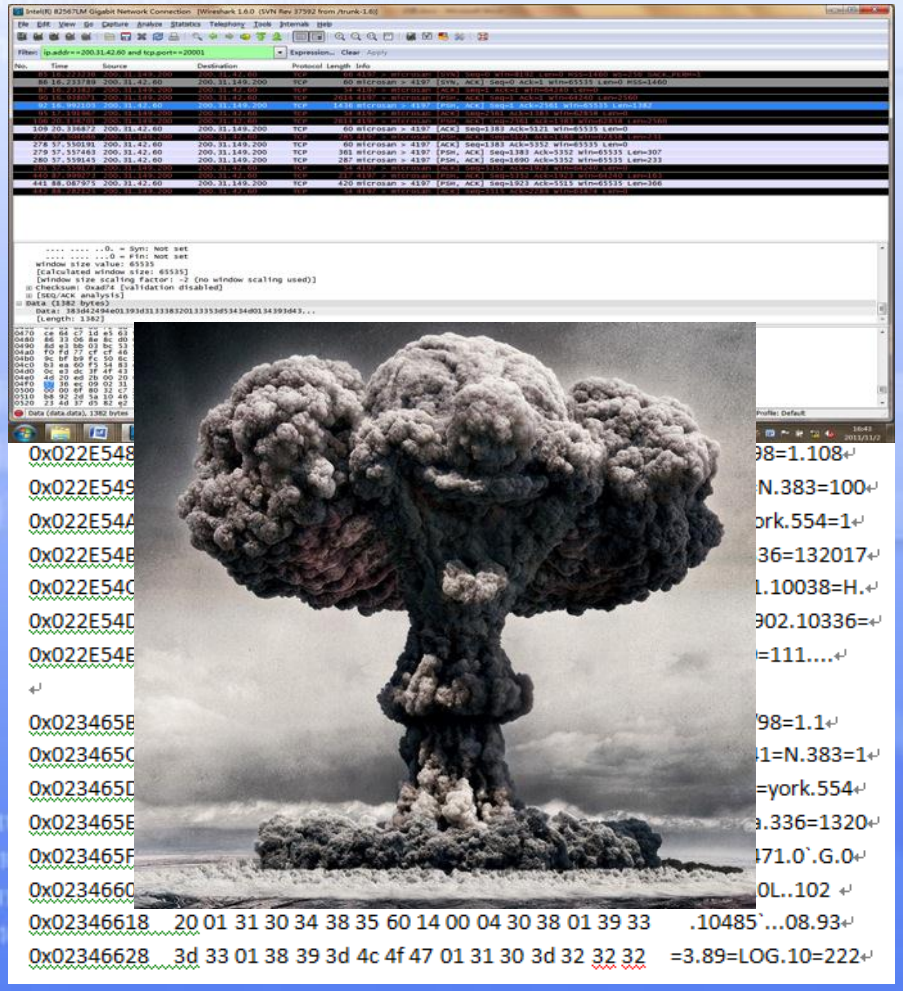
二代盾无盾注册/转账



由于银行在进行数据签名时，没有加入随机数，无法做到签名数据的唯一性，导致黑客预签数据，发送预签签名数据，达到二代盾无盾注册和转账的功能。

电子银行深度测试

案例四：加密协议破解、认证绕过



通过网络抓包，逆向分析，可以破解通信协议，绕过认证。黑客只需要在网络端抓取一次登录数据包，即可完全破解某交易中心的客户端认证系统，并且伪造任意机构间的交易。即可实现任意买卖的欺诈行为。

黑客可以为所欲为，后果很严重！

电子银行深度测试

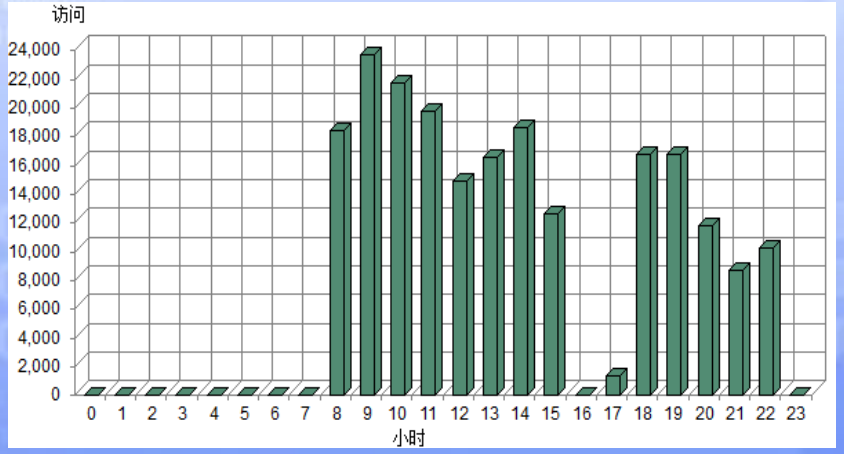
漏洞展示

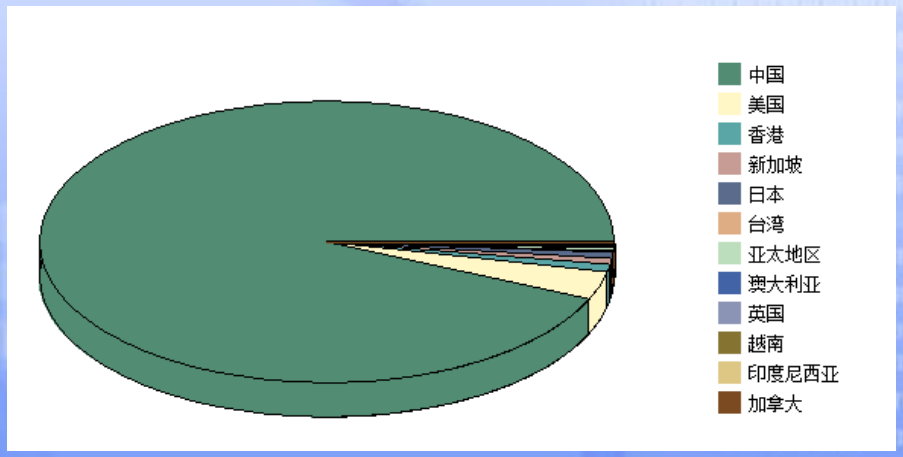
电子银行深度测试

从几个案例看

案例一：DDOS攻击溯源

2013年某月某日，某银行遭到DDoS攻击，攻击从下午一直持续至凌晨，期间网站一度无法打开。





本次攻击带来了超过250G流量，直接导致服务器网络堵塞。攻击IP遍布全球，除了国内IP外，美国、新加坡等也是主要攻击源。

通过大数据溯源网络攻击

从几个案例看

案例一：DDOS攻击溯源

附 1：下午攻击 IP TOP 100

按攻击次数排序，第一列为攻击次数，第二列为攻击 IP：

506	200.58.88.249	玻利维亚	CZ88.NET
329	130.193.129.85	伊拉克	CZ88.NET
300	117.204.201.80	印度	CZ88.NET

附 3：晚上搜索页攻击 IP

7078	8.35.200.34	美国	科罗拉多州布隆菲尔德市 Level 3 通信公司
6934	8.35.200.36	美国	科罗拉多州布隆菲尔德市 Level 3 通信公司
6484	8.35.200.37	美国	科罗拉多州布隆菲尔德市 Level 3 通信公司
6379	8.35.200.39	美国	科罗拉多州布隆菲尔德市 Level 3 通信公司
6247	8.35.200.38	美国	科罗拉多州布隆菲尔德市 Level 3 通信公司
6111	8.35.200.32	美国	科罗拉多州布隆菲尔德市 Level 3 通信公司

日期	恶意 IP	攻击网站	攻击方式
2013-05-23	61.135.152.209	gaoguai.net	远程代码执行
2013-05-28	210.70.250.202	gaoguai.net	远程代码执行
2013-06-30	222.124.3.153	www.tsjx.org.cn	异常 HTTP 方法探测
2013-06-29	8.35.201.54	pbbs.lnfisher.com	敏感文件探测
2013-07-18	8.35.201.53	www.chnam.com	Struts2 远程命令执行漏洞攻击
2013-07-21	8.35.201.52	sdqd.eloancn.com	Struts2 远程命令执行漏洞攻击

1，互联网攻击行为往往不是孤立的，攻击者通常会频繁的攻击多个目标。

2，通过关联多次攻击事件，分析攻击者常用攻击手段、攻击工具、发起地址、攻击类型等行为特征，可以为攻击者贴上标签。

3，将此次DDoS事件的攻击特征与以往恶意攻击者特征相匹配，即可定位攻击者身份。

通过大数据溯源网络攻击

从几个案例看

案例二：大规模网银钓鱼分析

攻击方式：不法分子以广播短信的方式诱骗用户上钓鱼网站骗取帐号密码。

转账需要：帐号+密码+动态密码

攻击成本分析：
构建网站成本+法律风险成本（？）
某银行网银用户总量m（几百万-3000万）
随手机用户总量n（5亿个手机）
上当的概率p（万分之一）
一条短信价格a（5分）

钓一条鱼成本

$X=a/(p*m/n)+?$

从几个案例看

案例二：大规模网银钓鱼分析

有人说过这么句话：
如果有10％的利润，资本就保证到处被使用；
有20％的利润，资本就活跃起来；
有50％的利润，资本就铤而走险；
为了100％的利润，资本就敢践踏一切人间法律；
有300％的利润，资本就敢犯任何罪行，甚至冒绞首的危险。

年份	2009年	2011年
用户量	800万	3000万
钓鱼成本	3.1万	0.83万

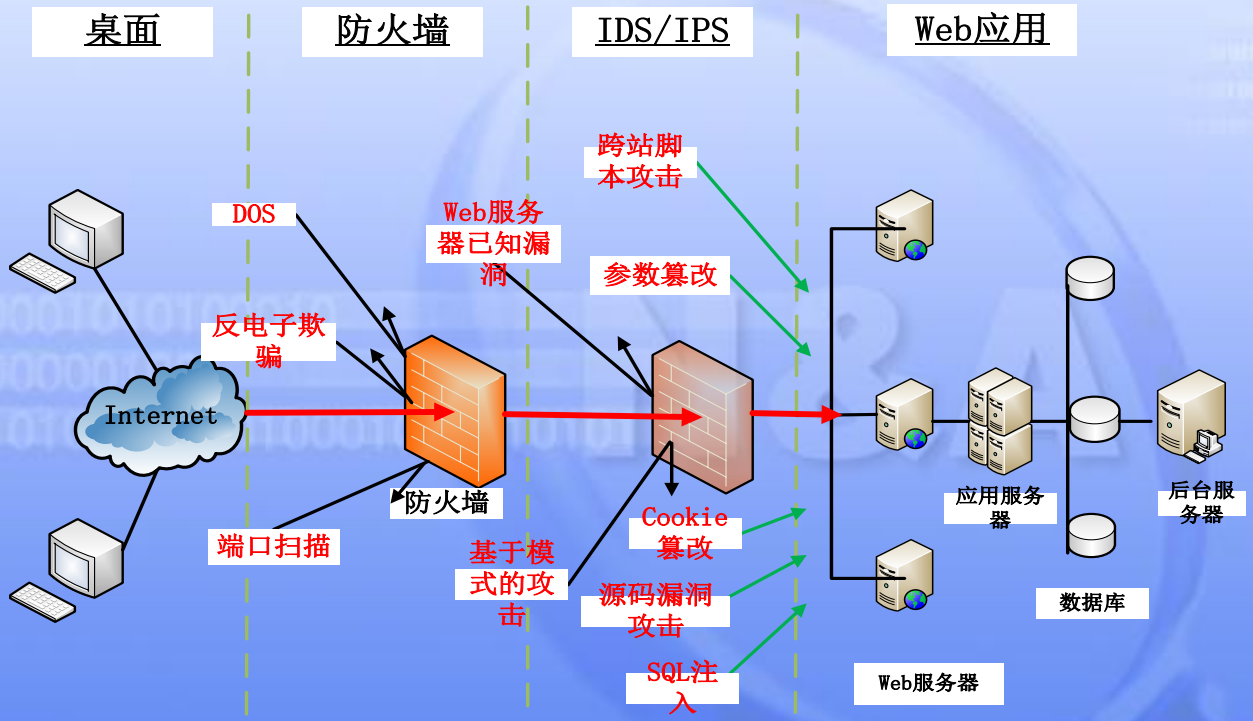
结论：
在2011年，不法份子赶冒一切风险钓鱼的条件是网银账户平均资金>0.83*300%=2.5万

攻防不仅仅是技术对抗，更是利益对抗

APT攻防之道

技术防控演进 —— 传统竖井式防御体系

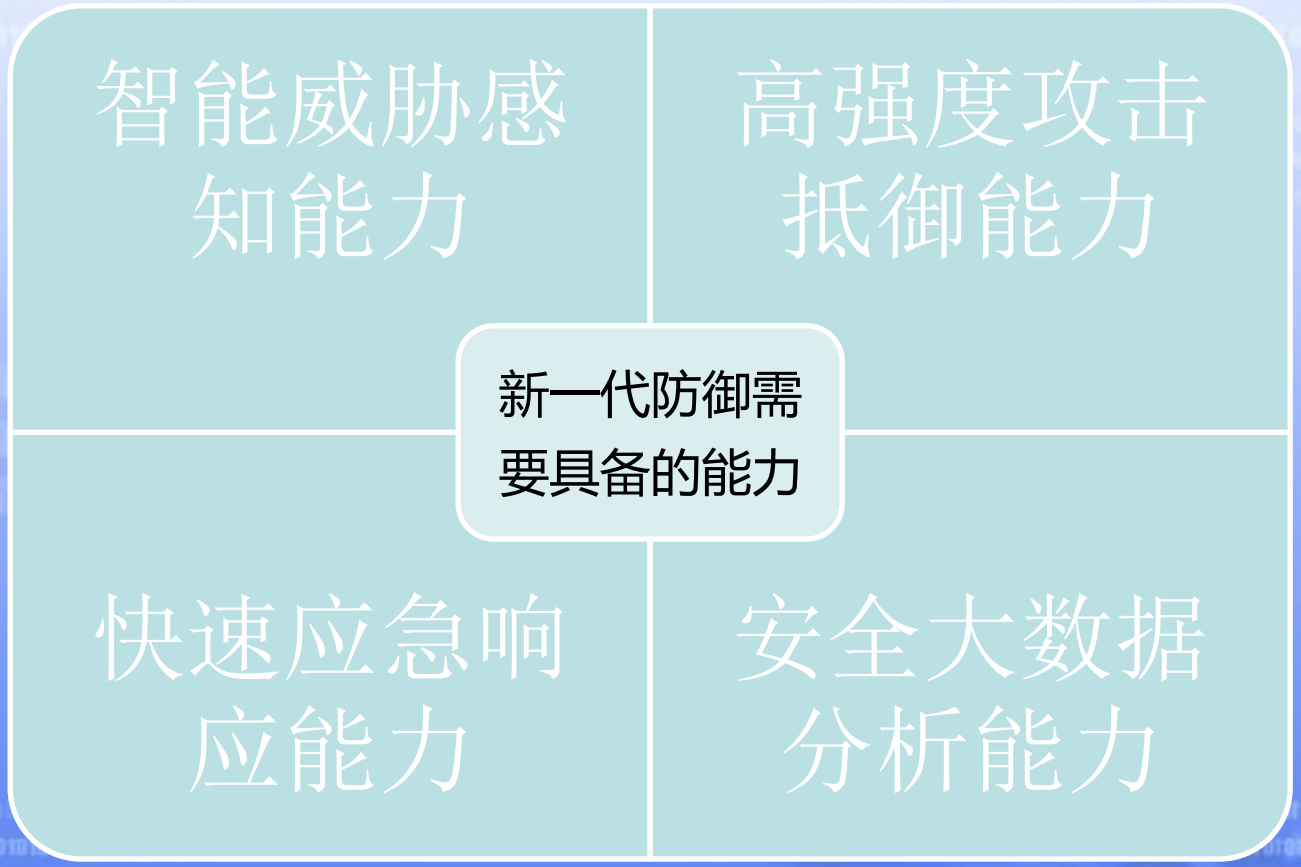
现状：以网络安全思路应对应用安全漏洞



基于边界保护和签名技术的防御体系存在滞后、错报漏报等局限，攻击者只需要抓住程序的一个漏洞点，即有可能入侵系统。

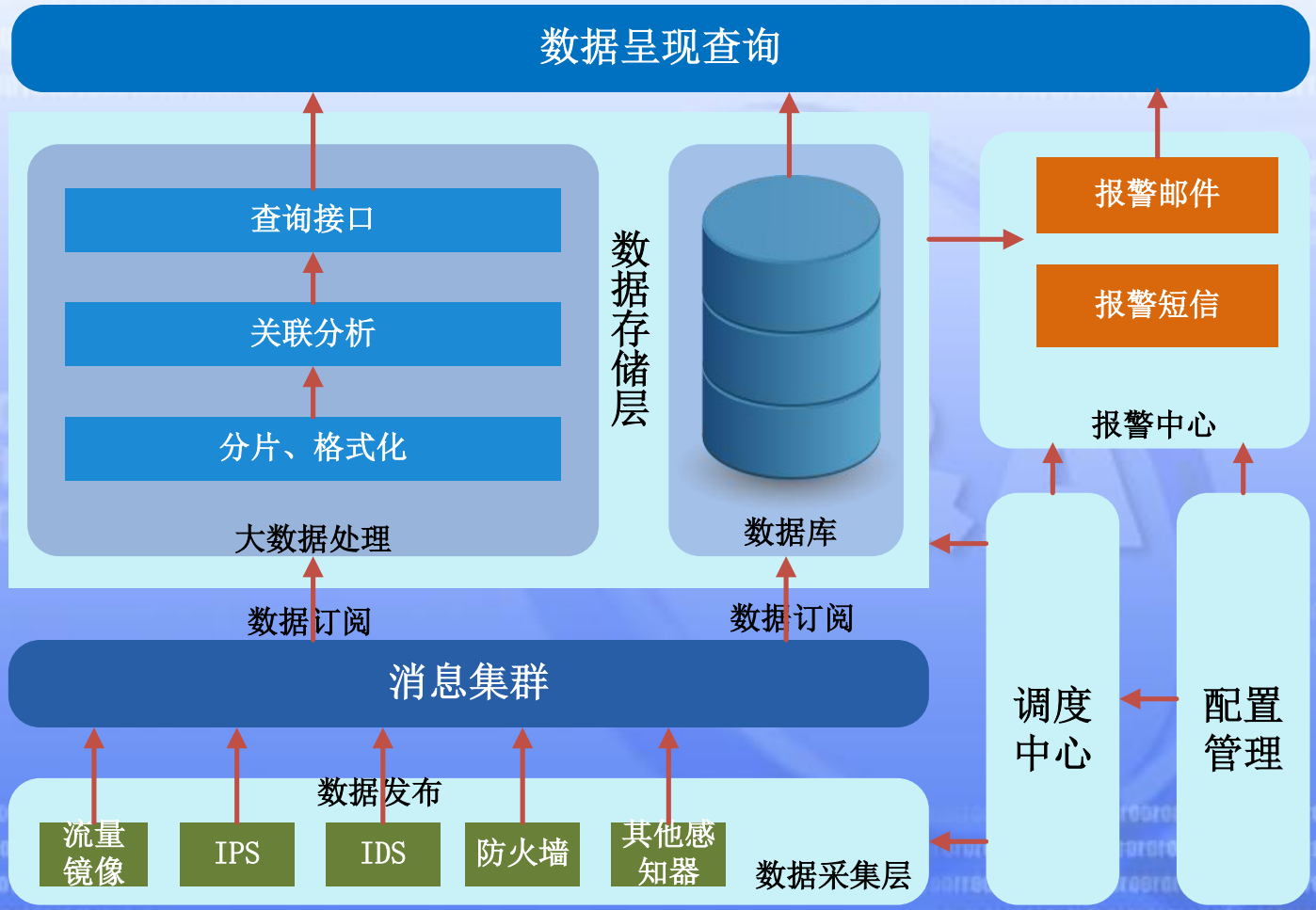
APT攻防之道

技术防控演进



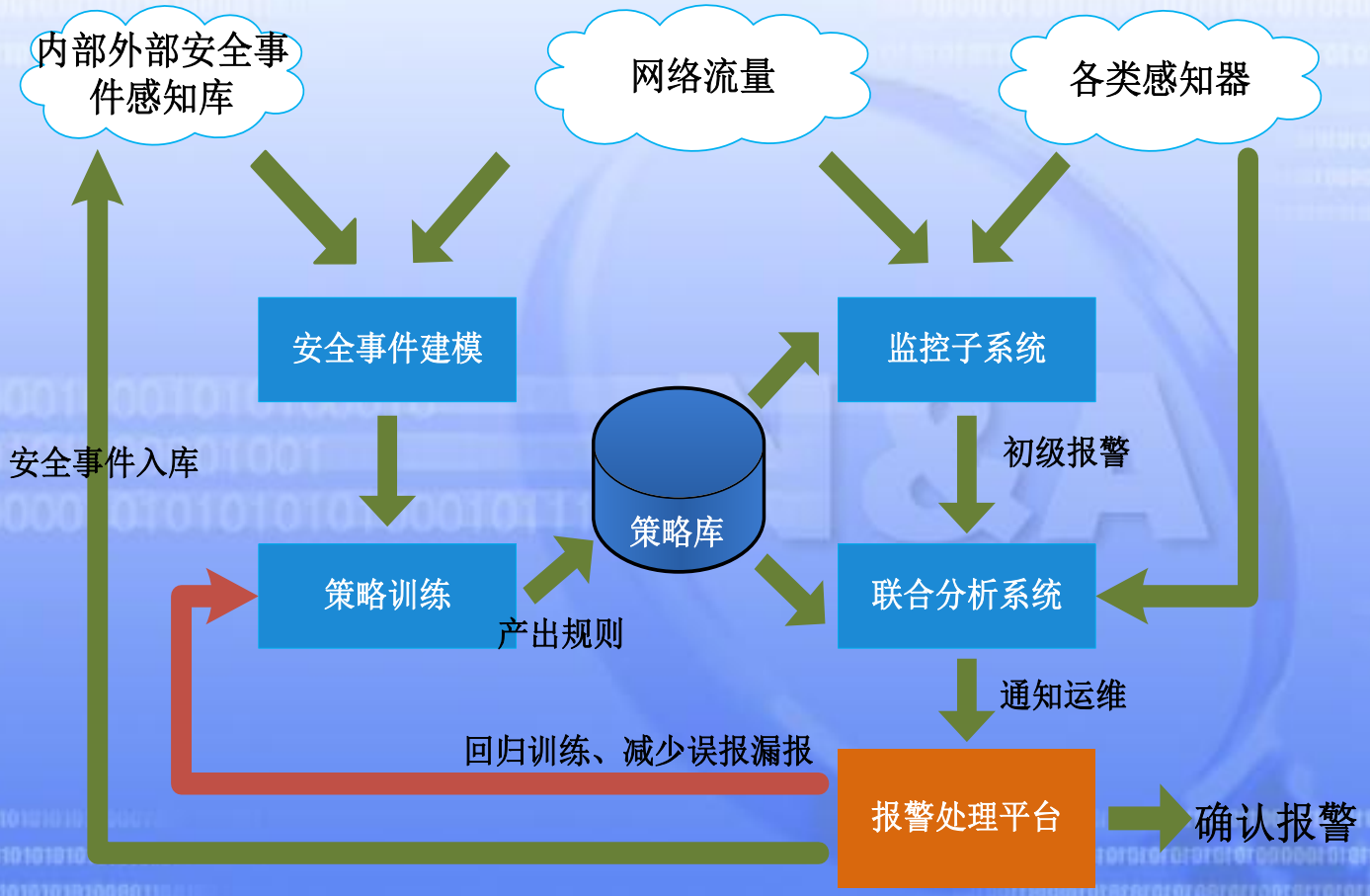
APT攻防之道

技术防控演进 —— 大数据的联合防控



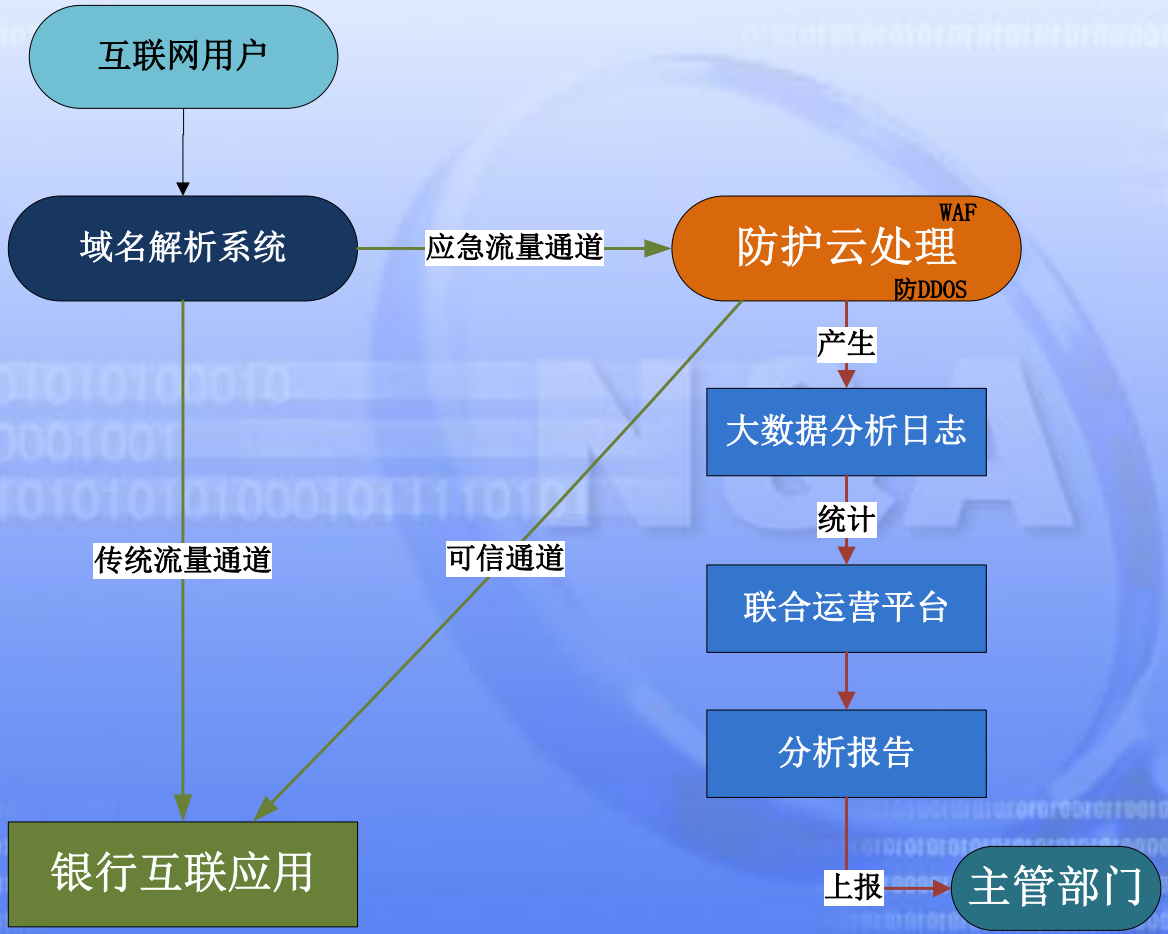
APT攻防之道

技术防控演进 —— 安全事件分析示意图



APT攻防之道

技术防控演进 —— 金融行业的联合防控



APT攻防之道

业务防控演进 —— 安全VS便捷

06年，静态密码保护（0安全成本）

08年，控件，软证书（每年每人1元）

10年，硬证书，动态密码（每年每人10元成本）

12年，二代证书，短信（每年每人30元成本）

14年，手机支付，互联网金融

APT攻防之道

业务防控演进 —— 风险控制体系

APT攻防之道

互联网金融时代

- 覆盖存、贷、流通各个层面
- 安全问题跨平台、跨地域
- 安全VS便捷

- 高度关联依赖的数字金融网络
- 业务的竞争与安全的合作
- 黑色产业猖獗与安全的正能量
- 保护消费者利益，维护金融稳定

一个故事关于

￥100万

APT攻防之道

caoyue@bslab.org