



专题:业务平台安全

通信业用户信息安全事件分析与防护

王 荣¹, 李 洪², 金 璇¹

(1. 中国电信股份有限公司江西分公司 南昌 330046;

2. 中国电信集团公司网络运行维护事业部 北京 100032)

摘 要:通过分析通信业发生的几起典型用户信息安全事件,研究目前用户信息安全存在的威胁,归纳总结问题原因,并从用户信息保护、安全技术手段、敏感信息保护、安全管理体系等几个方面提出解决办法,为制定通信业用户信息安全体系提出建设性的意见和建议,对通信业而言,具有可实施性和一定的实用价值。

关键词:信息安全;用户信息;安全体系

doi: 10.3969/j.issn.1000-0801.2013.08.013

Analysis and Protection for Information Security Event of Communication Industry User

Wang Rong¹, Li Hong², Jin Xuan¹

(1. Jiangxi Branch of China Telecom Co., Ltd., Nanchang 330046, China;

2. Network Operation & Maintenance Division, China Telecom Corporation, Beijing 100032, China)

Abstract: Some security incidents of user information were analyzed and the existent leaks were studied, the cause of the problem was summarized. The solution was put forward by analyzing from several aspects, like the user information protection, security technical means, sentimental information protection, security management system. Some constructive opinions and suggestions for the establishment of communication industry user information security system were put forward. It is practical and valuable for communication industry.

Key words: information security, user information, security system

1 引言

近年来,我国的信息通信技术得到快速发展,不仅改变着人们的观念、生活方式和工作方式,也改变着企业的观念和经营方式。通信业务系统积累和掌握了大量的用户信息,主要包括客户信息、账号、资金、服务使用等信息,与此同时,通信服务提供商所拥有的用户信息被他人不正当利用甚至非法窃取的危险性也越来越高,且用户信息泄露事件屡次发生,账号被盗用、信息泄露、垃圾短信等用户信息安全问题引起了社会大众的关注,通信服务商如何确保用户信息的安全管理、不泄露,形成了对通信服务商的巨

大挑战,这意味着对用户信息安全的研究被提上日程。

2 用户信息安全事件

根据工业和信息化部公布的《电信和互联网用户个人信息保护规定》,用户个人信息指“电信业务经营者和互联网信息服务提供者在提供服务的过程中收集的用户姓名、出生日期、身份证件号码、住址、电话号码、账号和密码等能够单独或者与其他信息结合识别用户的信息以及用户使用服务的时间、地点等信息”。

近期披露在媒体上的各种用户信息泄露事件层出不穷,而且至今还在不断的发展过程中。

2010年8月某运营商内部员工勾结私家侦探倒卖用户信息,运营商员工获刑。

2011年11月,某运营商的代理商利用掌握的用户信息进行商业广告短信群发获利被曝光。

2012年9月,部分通信服务提供商 Wi-Fi 的账号密码被盗用,导致部分用户费用增加,用户投诉增加,部分账号已在黑市上流通。

2012年12月,某运营商深陷“充值卡无效门”风波之中,安徽、广东、陕西、吉林等地的商户反映其在网上营业厅购买的电子充值卡出现失效问题,系登录账号密码被盗,盗号者通过获取充值卡账号和密码牟利。

2013年6月,中国电信网络安全中心发现,宽带家用无线宽带路由器中的 DNS(域名解析服务)配置可能被黑客篡改,从而造成用户个人重要信息泄露。

2013年6月,美国情报部门前雇员斯诺登表示,美国国家安全局持续入侵中国多家主要电信运营商网络,获取手机短信信息。

以上事件暴露出的用户信息安全问题很可能只是冰山之一角,因为从信息利用的角度,非法取得大量用户信息的人,为获取不正当利益会进行各种非法活动。

这些非法行为严重侵害了用户的权益,常常具有如下特点:

- 受损用户面广,用户不容易发现或损失金额小,易于逃避法律追究;
- 通过隐蔽的方式进行攻击或非法操作,以逃避打击与追踪;
- 通过网络进行交易,获利者隐于背后。

3 用户信息安全面临的问题及需求

作为直接面向用户的通信服务提供商,不仅面临用户投诉及费用损失,最大的冲击应当是由于用户对通信服务商的信任危机,导致企业名誉受损、公信力降低、服务可用性破坏、系统控制权丧失。

3.1 用户信息安全面临的问题

“前事不忘,后事之师”,从上述事件来看,用户信息安全可以归咎于安全管理与安全技术两方面的问题。

(1)管理方面

- 高权限账号被滥用引起高危操作,导致内部操作人员违规获取、篡改相关信息;
- 敏感信息缺乏模糊化处理,导致信息明文可见;
- 业务系统存在业务操作缺陷,导致信息易获取;

- 信息安全意识不高,采用弱密码或默认密码,导致被黑客破解利用。

(2)技术方面

- 业务系统安全域缺乏规划,导致安全问题容易扩散;
- 对信息非法访问缺乏审计监控,导致泄露源头无法溯源;
- 业务系统存在安全漏洞,导致易被入侵网络内部;
- 业务系统入侵检测能力不足,导致信息泄露难以及时发现。

3.2 用户信息安全问题的原因

从上述通信服务提供商面临的的安全管理与安全技术问题来看,可以归纳总结为个人信息保护意识不高、技术防护手段不足、敏感信息安全防护薄弱以及安全管理体系不完善4个方面原因,具体如下。

(1)个人信息保护意识不高

- 通信用户安全意识薄弱,没有树立正确的防范意识,视信息安全为通信服务商的责任,如诸多通信服务采用了弱密码,缺乏有效的安全预防措施。
- 信息安全常常从内部途径被泄露,作为通信服务商亦急需提高人员安全意识,加强内部宣传教育及制度管理,担负起维护信息安全的责任。

(2)技术防护手段不足

有些安全管控措施的落实,单凭制度约束是很难的,尤其是制度与其人员自身利益冲突,且违反制度的成本极低,或其不当行为不易被发现的情况下。缺乏有效、强制性的防护、监控、审计措施,不能保证用户信息安全的切实落地和执行。

(3)敏感信息安全防护薄弱

对敏感信息的产生、存储、使用、销毁等各个环节缺乏全生命周期管理,如业务系统安全生产区与办公、厂商、VPN 远程接入缺乏隔离,无法控制敏感数据的传播等。

(4)安全管理体系不完善

安全管理体系缺乏有效的测量、改进机制,缺乏系统的测量指标、方法,无法发现执行中的问题,由此就不能对其进行分析、改进和提升,也不能保持安全管理体系长期、有效。

4 用户信息安全保护思路

作为通信服务商要全面解决用户信息安全课题,应针对上述原因,从个人信息保护、敏感信息安全、技术防护手段以及安全管理体系等角度出发,分析用户信息安全保护思路。图1为安全防护思路策略。

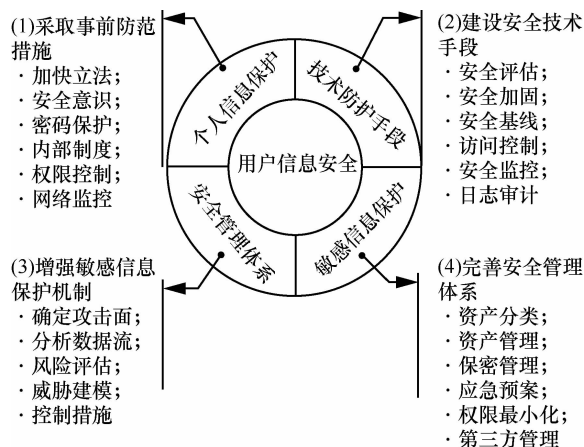


图1 安全防护思路策略

- 个人信息保护:个人信息保护要从源头抓起,可以采取一些事前防范的规避措施手段,如加强安全意识、用户访问控制、严格内部制度、加强网络监控等。
- 安全技术保护:加强应用层、系统层、网络层、物理层的安全防护,按照重要性等级分级进行安全评估、加固与维护,沿着威胁攻击路径部署安全措施。
- 敏感信息保护:基于业务流程,通过梳理归纳敏感信息的流转路径,明确业务数据的接续、数据处理过程,识别敏感信息潜在的泄露途径、位置,采用有针对性的控制措施。
- 安全管理体系建设:采用过程方法,完善体系建设,保障安全管理流程、管理目标的实现。

4.1 个人信息保护方案

个人信息保护最好的办法是防患于未然,事前防范措施是为了规范用户个人信息处理,具体如下。

- 加快个人信息保护的立法,从法律上提高非法侵权行为的成本。
- 提高个人安全保护意识,使用户了解信息泄露的危害、信息安全保护必要措施、出现信息泄露如何处理等,树立足够的自我防范意识,从而避免个人信息泄露和欺诈。
- 对用户个人访问权限进行严格认证和控制。例如,对用户身份认证进行短信确认、简单弱密码识别、客户警示语提示等。
- 加快企业内部制度管理,完善个人敏感信息保护制度框架。例如与业务合作伙伴签署用户信息安全保密协议,电子版资料是否严格限制查阅权限等。
- 加强网络安全监控是用户信息安全防护的重要手段,如及时发现仿冒与伪造的钓鱼网站。

4.2 安全技术保护方案

(1)安全加固

沿着威胁攻击路径部署业务系统的防御措施,由高至低地分别在应用层、系统层、网络层、物理层等采取相应的防护手段,提升业务系统安全防护能力。图2为业务系统安全加固措施示意。

(2)安全基线

为避免出现信息安全短板现象,对业务系统安全配置采用统一的基线标准,通过业务层面将不同安全防护要求逐层向下分解到对应的应用系统、数据库、操作系统、网络设备等不同设备和系统模块,为标准化和自动化操作提供途径。图3为业务系统基线安全模型。

安全基线可分为3个阶段实施进行。

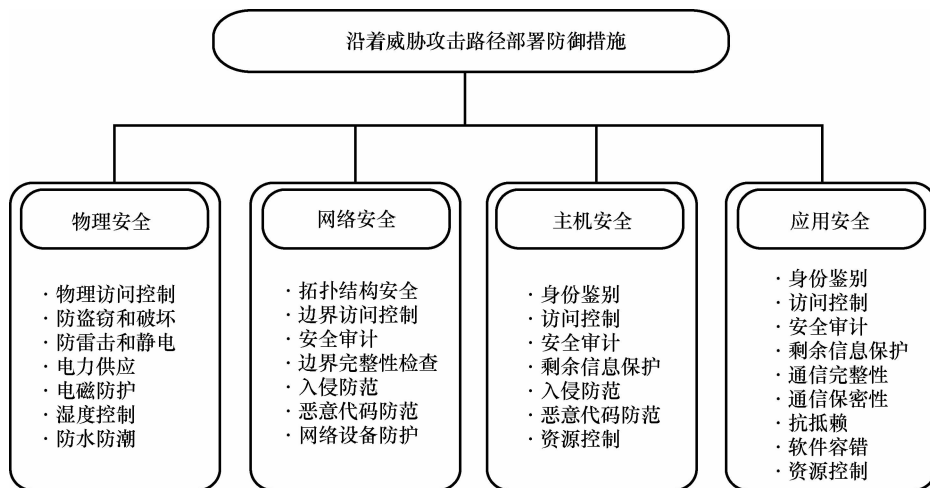


图2 业务系统安全加固措施

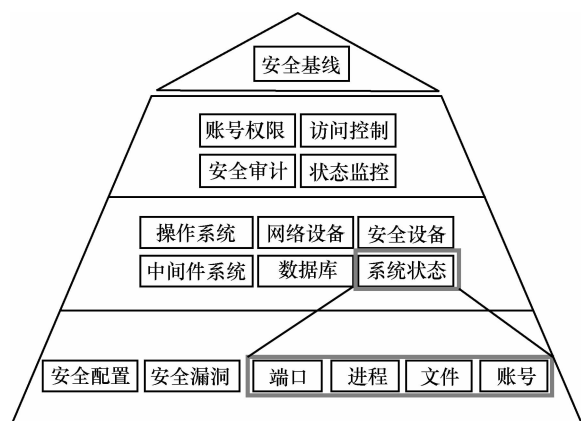


图3 业务系统基线安全模型

- 标准规范阶段。通过基线安全评估以确定应用系统安全状态、安全需求、合规要求,构建一套针对通信业特定业务系统的安全基线(检查项),结合安全加固工作规范实施安全配置,为后续标准化的技术安全操作提供框架。
- 配置工具阶段。由于应用系统庞大,分布广泛,信息安全基线管理需要自动化检查工作,以帮助安全基线管理的实施,通过开发、上线配套的安全核查工具,为自动化的技术安全操作提供支持。
- 流程建立阶段。业务系统在研发、验收、第三方入网、合规性安全检查、日常维护等各个流程设计安全检查环节,依据安全技术与管理标准,参照以往的安全事件和经验,选择和实施安全措施来控制安全风险,持续完善设备安全配置。

图4为安全基线实现的项目过程。

(3)安全配置规范

配置的安全对于提高业务系统的安全性起着非常重

要的作用,通常业务系统软件、网络设备、系统平台等基础设施存在配置漏洞,包括不必要的服务、共享连接、权限设置、口令等方面内容,反映了系统自身存在薄弱环节。业务系统依据“集中部署、分层防护”的原则,对业务系统内部进行划分安全域,简化防护边界,对重点关键业务系统,采取“重点系统、重点防护”的策略,因此在标准化安全基线内容时,安全配置规范是值得关注的重点。图5为安全配置规范。

(4)终端安全

以“主动防御”理念为基础,通过安全管理、桌面管理、数据保护、准入控制、主机审计等技术手段对内部的终端进行保护,实现操作系统加固及信息系统的自主、可控、可管理,保障终端系统及数据的安全。图6为终端安全保护系统。

4.3 敏感信息保护方案

要实现敏感信息的防护,应基于业务流程,通过梳理、归纳敏感信息的流转路径,明确业务数据的接续、数据处理过程,识别敏感信息潜在的泄露途径、位置,采用有针对性的控制措施。

基于上述思路,可以将敏感信息保护划分为如下5个主要阶段。

第1阶段:确定敏感信息保护评估的范围和边界。

第2阶段:从信息平台分析技术数据流。

从提供敏感信息的申请、审批和结果交付等功能的业务系统入手,通过细粒化的分析得到业务系统承载的全部技术数据流,并在此基础上,针对每一条数据流从网络、系统、应用、数据等不同层面,深入挖掘、识别和分析潜在的安全风险。

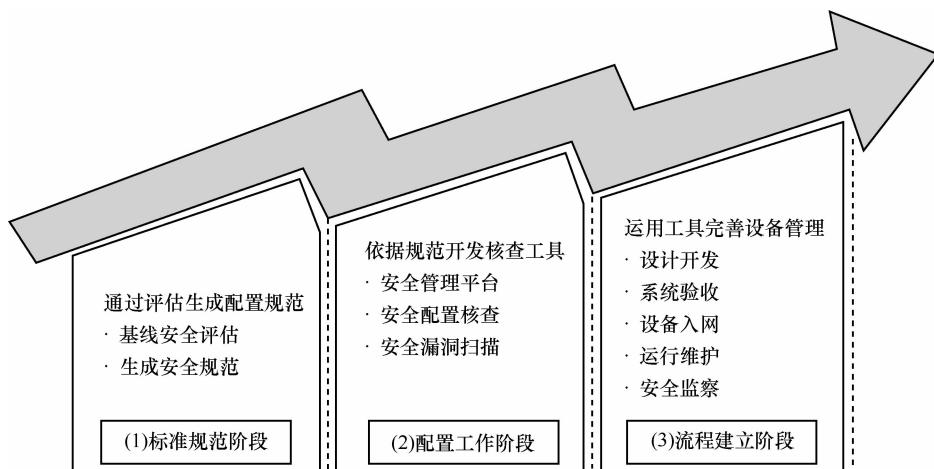


图4 安全基线实现的项目过程

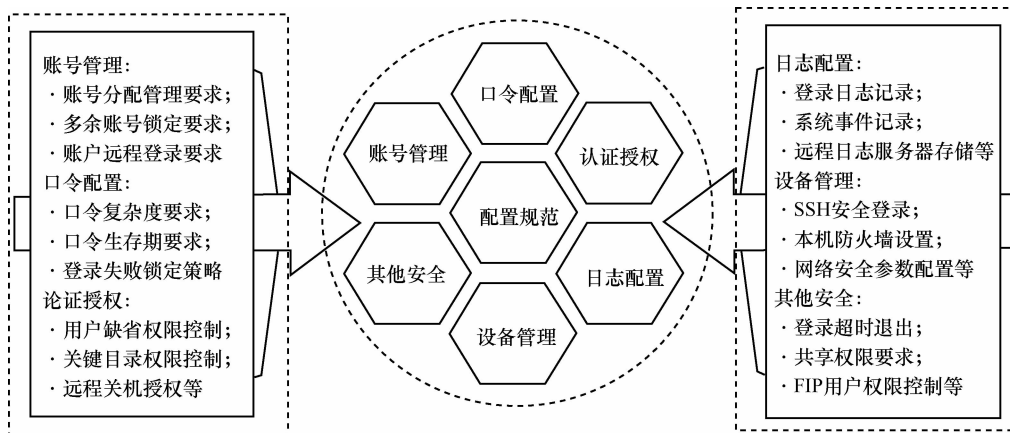


图5 安全配置规范

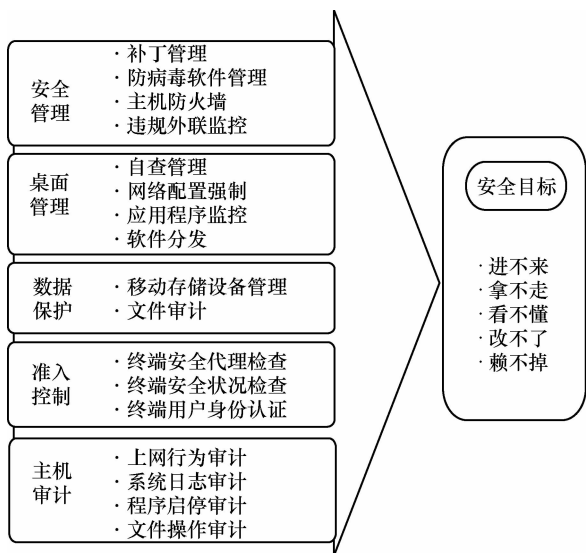


图6 终端安全保护系统

表1 敏感信息评估

序号	控制流程	控制要求
1	数据申请	有明文件的申请流程 在表单中根据集团的要求明确信息的敏感性 在表单中明确数据使用范围和时间 在表单中明确数据使用者(系统、部门、人员) 数据索取每次都通过申请并记录登记
2	数据审批	有明文化的审批流程
3	数据获取	对于获取数据的类型和级别有进行明文规定
4	数据传递	有明文化的传递流程
5	数据保存	确定对于系统存储的电子数据的保护程度
6	监督管理	制定了敏感数据的管理和使用规定

流程,采用适宜的方法、工具和手段降低风险,其中人员是根本、流程是核心、手段是支撑。要使安全管理体系有效发挥作用、起到实效,还必须实现如下几点。

- 全面化:要针对评估中发现的问题,应覆盖人员和组织、制度和流程、技术手段等所有要素,覆盖信息通信系统的整个生命周期,覆盖管理的整个过程。
- 系统化:管理体系应符合规划、实施、检查、改进思想,必须要有测量、反馈机制,能够进行内部监督、审计,形成正向的内部激励机制,不断进行改进和完善。
- 流程化:制度是有益的、必须的,但还必须贯穿部门间壁垒的、目标可控、易于落地的流程。流程使人员不需要过多的制度,只需按照流程工作即可,减轻了人员负担。
- 规范化:对于具体工作,必须给出明确的工作指导和表单,规范人员的操作行为。

第3阶段:从业务过程提炼业务数据流。

梳理与敏感信息有关的业务过程,并将业务过程与技术数据流进行匹配,描绘系统的业务数据流。同时,在业务数据流图上清晰标注敏感信息在业务数据流中的流转和存储情况,深入挖掘业务数据流中的业务风险。

第4阶段:技术业务两层面评估控制能力。

根据在第2阶段和第3阶段对技术数据流和业务数据流的分析,归纳数据申请、审批、获取、传递、保存和监管6个方面的控制评估情况,从而得到整体保护的评估能力评价。

第5阶段:敏感信息控制实现。

选择敏感信息控制的目标,并采用有效的管理、技术手段进行保护,如表1所示。

4.4 安全管理体系方案

安全管理的本质就是人与事的关系,是人根据制度和

(下转第118页)



的 D-S 证据理论。在原 D-S 证据理论的基础上,对证据冲突导致融合规则失效的情况,修正了融合规则对应的计算式;在 BPA 函数的构造中,对各证据源按信任度进行加权,同时利用模糊度计算式对不确定性进行预估,更好地区分了证据源的确定性与不确定性,保证了基础概率分配的精度。仿真表明,本文 D-S 证据理论进行合作频谱感知时无需主用户的参与和协助,且在 AGWN 和 Rayleigh 信道下得到的频谱感知性能较传统“与”融合、“或”融合及同类方法更好,可以作为认知无线网络频谱感知的通用方法,很好地适用于需要频谱资源共享的网络环境。

参考文献

- 1 Federal Communications Commission. Spectrum Policy Task Force. Rep ET Docket No 02-135, 2002
- 2 Carlos C, Kiran C, Dagnachew B, *et al.* IEEE 802.22: the first worldwide wireless standard based on cognitive radios. Proceedings of 1st IEEE Symp New Frontiers in Dynamic Spectrum Access Networks, Baltimore, USA, 2005
- 3 Zhao Q, Sadler B. A survey of dynamic spectrum access: signal processing, networking, and regulatory policy. IEEE Signal Processing Magazine, 2007, 24 (3)
- 4 Sun C H, Zhang W, Letaief K B. Cluster-based cooperative spectrum sensing in cognitive radio systems. IEEE ICC'07, Glasgow, Scotland, 2007
- 5 Stotas S, Nallanathan A. On the throughput and spectrum sensing enhancement of opportunistic spectrum access cognitive radio networks. IEEE Transactions on Wireless Communications, 2012, 11(1)
- 6 Yin W S, Ren P Y, Du Q H, *et al.* Delay and throughput oriented continuous spectrum sensing schemes in cognitive radio

- networks. IEEE Transactions on Wireless Communications, 2012, 11(6)
- 7 Han W J, Li J D, Liu Q, *et al.* Spatial false alarms in cognitive radio. IEEE Communications Letters, 2011, 15 (5)
 - 8 Peng Q H, Zeng K, Wang J. *et al.* A distributed spectrum sensing scheme based on credibility and evidence theory. Proceedings of the 17th Annual IEEE International Symposium on Personal, Finlandia Hall, Finland, 2006
 - 9 Nhan N T, Insoo K. An enhanced cooperative spectrum sensing scheme based on evidence. IEEE Communications Letters, 2009, 13(7)
 - 10 Vartiainen J, Hoyhtya M, Lehtomaki J, *et al.* Priority channel selection based on detection history database. Proceedings of the 5th CrownCom, Orlando, USA, 2010

[作者简介]



谢树京,女,梧州学院电子信息工程系电子信息工程专业教研室主任、讲师,主要研究方向为认知无线网络的频谱检测、频谱接入技术。



沈连丰,男,东南大学移动通信国家重点实验室教授、博士生导师,主要研究方向为无线通信技术。

(收稿日期:2013-05-14)

(上接第 84 页)

- 融合化:安全管理不是一个独立的体系,应与现运维管理、内部控制等现有制度和流程相融合,借鉴 PMP、ITIL、隐私数据保护等管理思想或方法的长处。

5 结束语

用户信息安全保护体系的建设并非一日之功,需要进行长期有序的建设和完善,随着下一代信息安全概念的提出和安全技术产品的不断完善,通信服务提供商通过强有力的管理组织领导、有效的激励措施,建立成功样板、问题发现和不断改进完善等方式,一定可以构建符合自己特点的用

户信息安全保障体系。

参考文献

- 1 王育民,刘建伟.通信网的安全——理论与技术.西安:西安电子科技大学出版社,1999
- 2 刘天华,孙阳,朱宏峰.网络安全.北京:科学出版社,2010
- 3 佟大柱.网络环境下的个人信息安全与保护探讨.网络安全技术与应用,2012(8):1009~6833
- 4 石玉春,张蕾.个人信息保护:互联网管理亟待解决的问题.中国通信业,2012(8): 1671~3060

(收稿日期:2013-08-01)