基于 HTTPS 的移动安全防护体系①

王成现, 李夫宝, 王 京

(江苏电力信息技术有限公司, 南京 210024)

摘 要: 随着移动互联网技术、无线网络技术以及智能化移动终端的不断发展, 移动交互平台已经成为企业信息化的重要标志, 然而面对日益严峻的网络安全威胁, 移动交互平台建设过程中必须充分考虑用户在接入或者使用过程中遇到的各种安全问题. 本文以江苏电力移动交互平台为研究对象, 结合公司业务特点, 提出了一种全新的移动安全防护方案, 确保移动交互平台的数据安全性、有效性以及通信链路的保密性, 满足了电力客户以及企业员工的移动交互需求.

关键词: 移动交互平台; 信息安全; 安全防护体系

Mobile Security Protection System Based on HTTPS

WANG Cheng-Xian, LI Fu-Bao, WANG Jing

(Jiangsu Electric Power Information Technology Co., LTD, Nanjing 210024, China)

Abstract: With the continuous development of mobile internet, wireless networks and intelligent mobile terminals, mobile interactive platform has become an important symbol of modern enterprise informatization. However, being faced with the increasingly serious network security threats, various kinds of security issues must be taken into full account in the process of the access and use, during the process of the construction of mobile interactive platform. Combined with the characteristics of the existing business, Jiangsu Electric mobile interactive platform is accomplished as an example in this paper to put forward a new mobile security program to ensure that the confidentiality of mobile interactive platform's safety, effectiveness and communication links. The platform meets the interactive demand of mobile for electricity customers and employees.

Key words: mobile interactive platform; information security; security protection system

1 引言

随着科技的迅速发展, 全球智能移动终端(包括智能手机、平板电脑等)出货量已经超过传统的 PC 机, iOS 及 Android 系统已经成为移动智能终端使用的主流操作系统. 移动终端的智能化, 人机交互界面的革命性发展, 计算机技术、无线网络通讯技术的发展与融合, 促使移动互联网成为主流的信息交互模式[1]. 企业移动交互平台的建设已经成为企业信息化的重要标志. 企业移动交互平台能使企业领导与员工只需一部移动终端设备即可随时随地利用网络便捷快速地处理企业内部日常工作, 实现高效办公与资源共享.

然而企业移动交互平台从严密防范的内网拓展到开放的外网时, 在移动终端接入的身份验证, 数据传输, 安全访问控制等环节, 敏感信息存在不同程度的安全隐患. 无线通信传输的开放性、灵活接入性以及平台功能应用的多样性同样会导致一系列影响移动终端安全性的问题, 例如恶意软件扩散、恶意网址链接入侵等. 企业移动交互平台面临的风险有: (1) 移动终端的遗失或者终端感染病毒以及恶意代码, 将导致用户敏感数据的泄露; (2) 数据传输的不安全性导致用户鉴别信息被攻击者利用, 移动业务应用的配置信息被破坏, 造成用户和业务应用敏感信息泄露、用户无法正常访问业

① 基金项目:国家科技计划基金(2013YQ240511)

收稿时间:2015-11-12:收到修改稿时间:2016-01-11 [doi:10.15888/j.cnki.csa.005276]

务应用的后果; (3) 部署在外网的平台运行模块受到木马、恶意代码等攻击, 将使移动用户接入或访问平台受到影响, 交互平台应用数据信息泄露等. 一般外网访问移动交互平台需要通过 VPN 网络或者 HTTPS 协议, 数据在网络上传输必须经过复杂加密才能保证信息安全. 有鉴于此, 为了更好的利用移动终端访问移动交互平台, 更妥善的解决企业移动交互平台访问的信息安全问题, 结合江苏电力移动交互平台, 本文提出了一种基于 HTTPS 的移动安全防护体系.

2 移动安全防护体系构建原则

(1) 有限应用原则

通过企业内部网络或者外网无线网络接入移动交互平台的用户只能对授权的应用业务进行处理以及管理服务操作.

(2) 网间隔离原则

企业的移动交互平台内部局域网络与外部网络必须相互隔离, 同时企业内部的业务管理网络也必须与外网隔离, 若要与外网连接则要通过专用对外接入的局域网才能进行接入.

(3) 单向访问原则

移动交互平台客户端采用单向访问限制的方式, 不允许用户通过移动交互平台与外网相连.

(4) 安全第一的原则

在移动交互平台网络架构设计中, 优先选择经过国家认证的 VPN 网关、防火墙、AP 等硬件设备等, 使用身份认证、数据加密等技术, 保证数据信息安全.

(5) 继承发展原则

构建移动安全防护体系应考虑移动信息化未来的安全需求和安全技术的发展因素, 选用的安全技术和设备应具备良好的可维护性和可扩展性.

3 背景知识

3.1 移动终端操作系统简介

目前在移动智能终端上使用的主流操作系统包括 Android(安卓)以及 iOS 等.

Android(安卓)是由 Google 公司和开放手机联盟领导开发的一种基于 Linux 的自由、开放源代码的操作系统. 目前被广泛应用于移动终端设备, 包括智能手机、平板电脑等. 全世界目前有超过 10 亿台设备采用此款操作系统. 在安全机制方面, Android 系统应用沙箱机制隔离进程资源、安全高效的内存管理技术和进程间通信机制来保证用户的数据安全[2]. 默认情况下, 所有应用都无权限对其他应用、系统或者用户进行较大影响的操作, 包括读写用户联系人、电子邮件等隐私数据, 读写其他应用文件, 访问网络或阻止设备待机等.

iOS 是由苹果公司为 iphone 手机设计开发的移动操作系统, 后来陆续供 ipod touch、ipad 以及 Apple TV 等产品使用. 在安全机制方面, iOS 专门设计的低层级的硬件和固件功能, 可以防止恶意软件和病毒; 高层级的 OS 功能, 确保企业数据和个人信息的安全. 同时 iOS 支持加密网络通信, 有助于保护传输过程中的敏感信息.

3.2 HTTPS 协议

HTTPS(Hyper Text Transfer Protocol over Secure Socket Layer)是最初由网景公司进行研发, 加入了安全套接字层(SSL)的 HTTP 加密传输协议, 是 HTTP 协议的安全版. HTTPS 协议需要使用经 SSL 加密传输的数据信息, 所以 HTTPS 协议的安全基础是 SSL. SSL 协议可以保证传输数据的保密性、数据完整性, 实现通信双方的互相身份认证. HTTPS 通过使用对称加密算法、CA 公私钥密码算法、摘要算法等, 加密强度可以达到 128 位或者以上[3]. HTTPS 协议主要解决客户端对服务器的身份确认、服务器对客户的身份确认、在服务器和客户之间建立安全的数据通道这三方面的问题. 采用 HTTPS 协议的服务器必须要有一套数字证书, 可以自己制作, 也可以向组织申请. 自己颁发的证书需要客户端验证通过才可以继续访问, 使用受信任公司申请的证书则可以避免上述问题. 这套证书的实质就是一对公钥和私钥.

HTTPS 是最为广泛使用的基于 PKI 的信任体系解决方案, 用来在客户端和服务器之间建立安全的 TCP 连接, 使用前要求在客户端先安装用户 CA 证书, 在服务器端安装服务器证书, HTTPS 具体工作流程如图 1 所示.

具体说明如下:

(1) 客户端向服务器端发出连接请求.

(2) 服务器端向客户端发送自己的认证证书以及证书的相关信息.

(3) 客户端验证服务器端发送过来的认证证书是否为信任的 CA 中心所签发. 若正确, 则继续执行协议,

若不正确, 则在客户端发出警告信息.

(4) 客户端生成随机的会话密钥, 并且使用服务器公钥对会话密钥进行加密, 发送到服务器端.

(5) 客户端对该会话密钥进行签名, 产生客户端签名.

(6) 客户端将自己的认证证书以及客户端签名发给服务器.

(7) 通过会话密钥、客户端签名、客户端证书验证客户端身份.

(8) 客户端与服务器端拥有相同的会话密钥, 双方身份确认, 双方可以使用此会话密钥对通信内容进行加密, 安全通信通道建立.

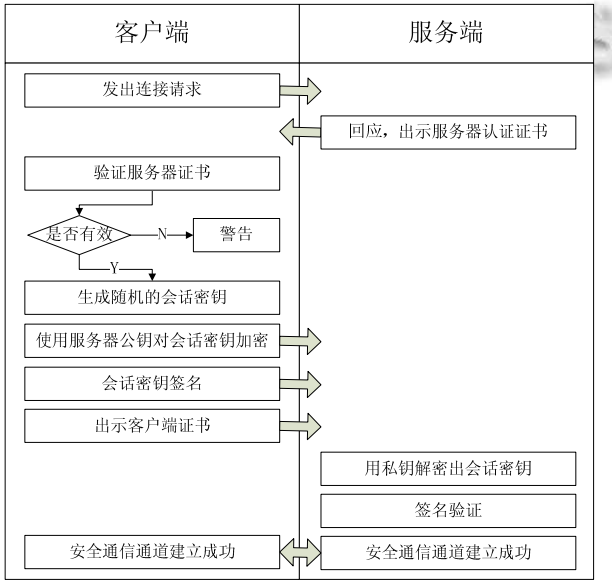

图 1 系统总体框图

3.3 CA 证书

CA(certificate authority)是数字认证中心的简称, 负责签发证书、认证证书、管理、废除已颁发证书, 是 PKI 系统通信双方都信任的实体. CA 具有合法性、中立性、权威性和公正性. CA 的主要职责是制定相应政策和具体步骤来验证、识别用户身份; 并且对证书的信息资料进行管理, 确保证书主体名称无重名现象; 在证书使用过程中检查证书的有效期; 对作废证书系统进行及时的发布与维护; 签发证书, 以防证书被篡改或者伪造, 检验证书持有者的身份和公钥的拥有权, 并且通过加解密的方法来实现网络数据交换的安全性[4][5].

目前 CA 证书可以利用免费的 Open SSL 软件包自动生成获得, 也可以由付费的 CA 证书认证中心获得. CA 证书的内容包括: 电子签证机关的信息、公钥用户信息、公钥、权威机构的签字和有效期等. 证书的格式和验证方法普遍遵循 X.509 国际标准.

4 移动交互平台基本功能框架

电力企业移动交互平台基本框架如图 2 所示. 该移动交互平台的主要包括移动客户端、外网运行支撑、数据库、内网运行管理, 实现对公司客服、营销、电力交易、金融等业务域的移动应用支撑.

对于内部员工用户, 移动交互平台主要提供待办提醒、邮件提醒、公司要闻等办公类信息, 方便员工的移动办公, 提高工作效率. 对电力客户, 平台提供查询电费、电量等营销、客服类的移动应用, 方便用户的用电生活, 提升客户满意度. 平台提供的移动商店实现了对各业务域的移动应用的聚合, 提供移动应用、客服业务应用、电力交易业务应用、金融业务应用等应用以便内部员工或者电力客户下载使用. 平台移动客户端支持 Android 和 IOS 主流操作系统. 各业务应用通过 HTML5 技术和平台提供的开发组件开发, 降低移动业务应用开发的复杂度, 提高开发效率.

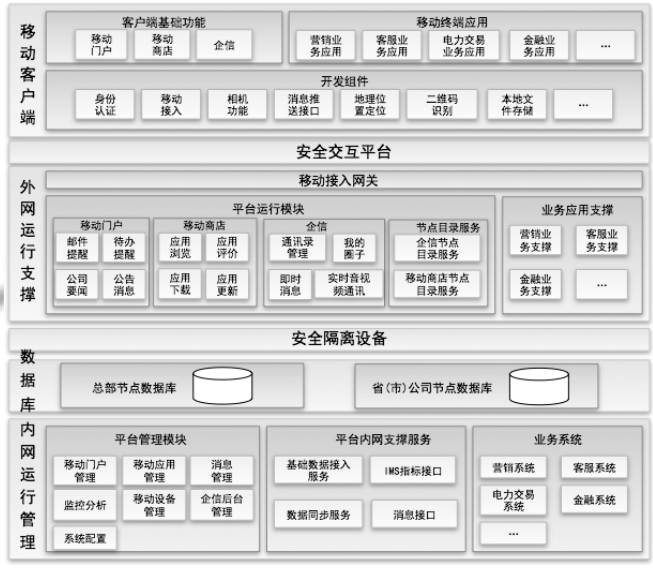

图 2 移动交互平台总体框架图

目前电力移动交互平台主要应用在外网. 移动终端使用移动网络或者无线网络, 通过防火墙、安全交互平台、移动接入网关、安全隔离设备, 结合 CA 证书, 通过 HTTPS 协议安全地对服务器进行访问. 应用场景如图 3 所示.

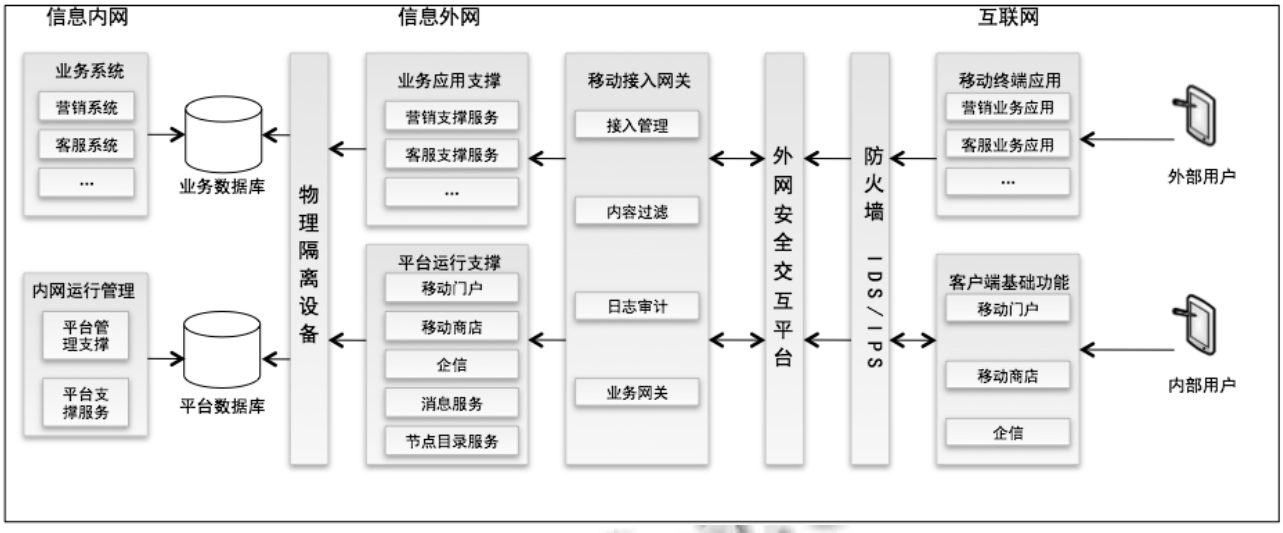

图 3　移动互联网应用场景

5　移动交互平台安全防护体系构建方案

鉴于移动交互平台提供的主体功能, 以下介绍基于 HTTPS 的移动安全防护体系的构建方案, 以保证移动交互平台在外网环境下的安全使用. 移动安全总体防护框架如图 4 所示.

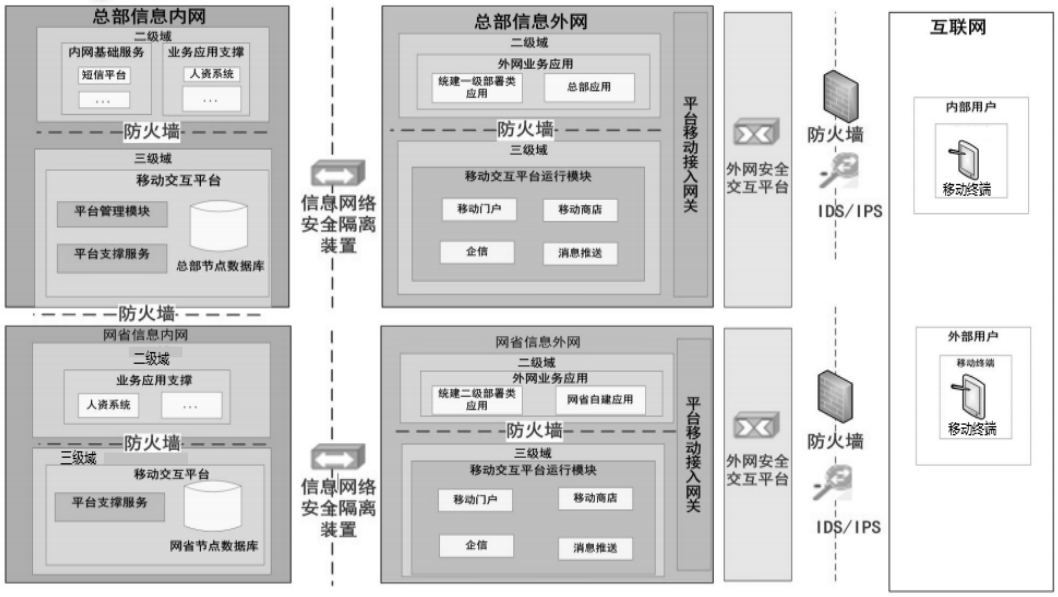

图 4　移动安全防护体系总体框架

本文所提出的移动安全防护体系构建方案是首先在移动终端客户端建立安全沙箱与隔离区保护数据与应用的安全, 在互联网与外网安全交互平台之间部署防火墙以及 IDS/IPS, 对不安全访问进行过滤与阻止. 通过在互联网与外网之间部署安全交互平台保障信息数据传输的安全. 然后通过移动接入网关进入信息外网, 使用移动接入网关接入信息内网可以使信息应用系统不暴露后端请求地址, 对后端服务器回显数据进行有效过滤, 充分保护应用服务的安全. 通过信息网络安全隔离装置访问信息内网, 最大限度的保证数据访问安全性.

5.1　移动安全防护方案

5.1.1　客户端安全隔离

在客户端建立安全沙箱以及隔离区. 安卓系统沙

箱的本质是为了实现不同应用和进程之间的隔离. 安卓系统通过使用 Dalvik 虚拟机和 Linux 的文件访问控制来实现沙箱机制. IOS 的沙箱运行机制是在 IOS 中, 每个程序对应到 APP 自己的一个目录, 这个目录只有这个应用有读写权限, 其他任何 APP 都没有这个目录的读写权限. 沙箱的作用就是保证 APP 数据的安全性, 沙箱的作用就是保证 APP 数据的安全性, 防止恶意软件、病毒等窃取信息. 借鉴传统的沙箱设计理念, 江苏电力移动客户端在开发时实现了应用程序运行容器, 该容器封装所有系统接口, 避免应用直接调用而引起的安全问题. 另外使用虚拟化技术建立虚拟文件系统 (VFS) , 使用独立的数据存储空间对所有应用进行独立存储, 同时限制应用访问路径, 应用仅能访问自己所在文件夹, 并且对应用和数据分别进行存储加密, 有效防止恶意软件篡改等安全问题.

5.1.2 安全交互平台

(1) 基于 CA 双向认证的安全通道建立

安全交互平台的作用是在终端与业务服务器之间建立安全传输通道, 在建立安全通道的过程中使用 CA 证书双向认证机制保证数据的安全. 安全通道建立流程如下: ① 交互客户端连接交互服务器, 通道建立请求; ② 交互服务器发送数字证书给客户端, 客户端根据预先导入的 CA 根证书进行网关有效性验证; ③ 交互客户端发送数字证书给服务器, 服务器根据预先导入的 CA 根证书进行网关有效性验证; ④ 客户端与服务器分别产生一份密钥因子; ⑤ 交互客户端与服务器采用非对称加密算法交互密钥因子, 产生加密通信所需的密钥; ⑥ 交互服务器发送访问控制策略列表给客户端; ⑦ 客户端建立数据转发代理, 完成通道建立流程.

(2) 数据加密传输

安全交互平台对所有通过安全专用通道传输的数据进行加密, 加密密钥在建立通道时动态协商, 并根据加密时间和加密数据量定期更新密钥, 加密算法支持国产 SM1、SM2、SM3 算法及 AES、3DES 等国际通用算法, 兼顾数据的保密性和传输效率. 安全交互平台除支持国际通用的 RSA、AES、3DES 等加密算法, 还支持国家密码管理局发布的国产 SM1、SM2、SM3 密码算法.

(3) 数字签名技术保证数据完整性

数字签名技术又称公钥数字签名、电子印章, 是保证数据传输认证成功的关键技术. 若签名属于伪造、假冒、更改, 则导致认证的失败[6]. 数字签名技术是非对称密钥加密技术和数字摘要技术的应用. 安全交互平台对所有通过安全传输通道的数据进行数字签名, 即交互客户端通过 SM3、MD5 等散列算法和 SM2、RSA 等非对称加密算法对交互网关服务器发来的数据进行校验, 反之, 交互网关服务器也通过同样的算法对交互客户端发来的数据进行校验.

(4) 数据的高效、透明传输

交互网关和交互客户端进行数据传输时, 采用数据压缩传输的方式, 极大地提高了业务数据的传输效率. 安全交互客户端为独立运行的应用程序, 初始化配置后, 运行时会自动进行安全通道建立和重连、双向身份认证、动态密钥协商和透明数据转发, 无论是专用业务客户端或网页浏览器, 都无需进行程序改造.

(5) 动态密码技术

动态密码技术是使用专用算法在需要的时候通过管理系统自动生成变化的随机数字组合, 每次使用的密码都不相同. 目前主流的产生形式有手机短信、硬件令牌、手机令牌, 动态密码的优点是跨平台, 使用便捷, 广泛应用于网银、网游、信息通信领域. 由于动态密码技术的安全性以及使用特点, 越来越多的企业采用动态密码技术保护其 VPN、服务器、网络设备等. 当用户利用 VPN 应用客户端连接到企业移动交互平台管理内部网络时候, 则安全网关将会从网络的 AD 服务器进行用户名信息检测, 如果检测到该用户名存在则会自动生成认证动态密码发送到其手机上, 并将手机上的动态密码输入到实时平台上从而完成整个登录过程[7]. 本防护方案中在移动客户端登录系统时, 采用动态密码技术, 从而提高信息安全程度, 有效的避免了密码信息被泄露的可能.

5.1.3 移动接入网关

目前企业移动交互平台的移动接入安全不仅要解决移动终端、互联网传输、移动应用、安全兼容等方面的安全需求, 更要重视移动接入作为一个系统整体的安全需求. 移动接入安全需求主要表现在数据的传输安全、支持多种安全接入方式、统一配置管理、网络边界划分以及相应的保护措施、适用的密码算法管理配置等[7].

本文所提出的移动安全防护方案使用移动接入网关保证移动接入的安全性. 具体方式是, 通过部署

NIGIX 为前置 HTTPS 服务, 把交互平台传输的 HTTPS 请求解析为标准的 HTTP 请求, 然后以反向代理的方式转发到 JAVA 程序, 再由 JAVA 程序数据校验后发给业务系统.

5.2 移动安全防护工作流程

移动安全防护体系工作流程如图 5 所示.

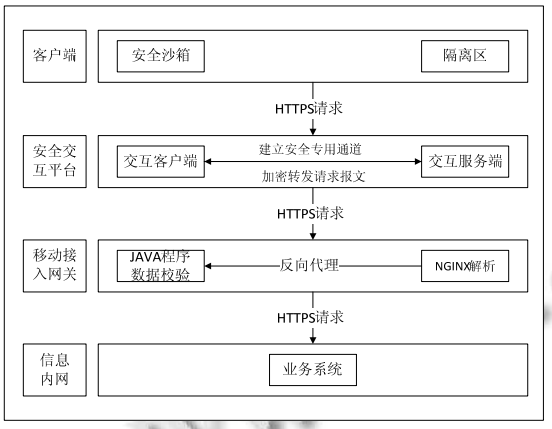

图 5　移动安全防护体系工作流程

具体工作流程如下: ① 客户端通过 HTTPS 协议向移动交互平台发送业务请求; ② 交互平台客户端与交互平台服务器建立安全专用通道; ③ 交互平台客户端对业务报文进行加密并转发到交互平台服务器; ④ 交互平台服务器将业务报文以 HTTPS 协议请求的方式转发到NGINX服务器; ⑤ NGINX服务器通过反向代理把业务传输到 JAVA 程序; ⑥ JAVA 程序进行数据校验后以 HTTP 协议转发到业务系统.

6　体系部署对平台的影响及应对措施

在部署安全防护体系时借鉴了大量资料, 对其中可能出现的安全防护体系对移动交互平台正常工作性能带来的影响进行相应的评估. 安全防护体系对移动交互平台的效率、性能等方面影响较小, 可以忽略不计. 我们可以采取如下措施: 一方面通过对用户进行评级, 对于不同级别的用户开放不同的权限减小数据的交互, 从用户角度来说, 基本感受不到交互平台性能对用户体验的影响. 另一方面还可以通过对必要的生物特征的识别允许安全防护系统对用户的安全信息进行记录(定期删除), 设置随机的生存周期, 在生存周期内, 可以略过之前的复杂的步骤, 提高性能.

7　结语

本文从移动交互平台在企业应用角度出发, 分析了移动交互平台应用背景以及面临的安全问题, 详细介绍了江苏电力移动交互平台在避免这些风险所采取的安全措施, 提出了一整套以 HTTPS 协议为基础的移动安全防护体系. 此移动交互平台防护体系方案部署灵活简单高效, 满足了电力客户以及企业员工的移动交互需求, 有效提高了移动交互平台使用的安全性. 本平台完全遵循国网公司各项 IAO 技术规范, 其安全部署架构适用于各家网省单位, 所依赖的基础平台均为国网统推系统, 具备在国网总部及各家网省单位推广的条件.

参考文献

1 刘峥,王静.移动办公在发电企业中的研究与应用.电信科学,2013,11(11):115-121.
2 朱筱赟,胡爱群,邢月秀,赵然.基于 Android 平台的移动办公安全方案综述.信息网络安全,2015,(1):76-83.
3 茹惠素.基于 HTTPS 协议的统一登录系统设计与实现.浙江工业大学学报,2008,(5):527-530.
4 吴晨刚,董恒竞,唐勇.基于移动终端的企业信息安全架构设计与实现.信息网络安全,2013,(5):83-85.
5 马斌.计算机安全技术在企业移动办公中的应用.科技创新导报,2013,(20):33-34.
6 刘金,甘睿.分析移动办公的网络安全技术方案.网络安全技术与应用,2014,(4):122-124.
7 王宏斌.企业移动办公的安全接入研究及实现[学位论文].郑州:郑州大学,2010.