一种基于 MSISDN 虚拟化的移动通信用户数据拟态防御机制

刘彩霞 季新生 邬江兴

(国家数字交换系统工程技术研究中心 郑州 450002)

摘 要 对于移动通信用户而言,作为其身份标识的 MSISDN 号码对外公开,而在移动通信网中,MSISDN 号码与用户其它数据项绑定关联存储、传递和使用,这也是移动通信用户信息泄露或者被恶意窃取的重要途径.通过深入研究移动通信网络架构、协议体系和业务提供模式,该文提出一种移动通信用户数据拟态防御机制.该机制的核心思想是通过在不可控的通信过程和网络设备中动态引入虚拟 MSISDN 号码,使 MSISDN 号码在传递、存储和使用等环节具有随机性和多样性,从而隐匿或者打破用户真实 MSISDN 号码与其它数据的关联关系,进而有效实现用户信息防泄露和防窃取.方法的特点是不改变现有移动通信网的协议体系,并能够保证用户对外公开的 MSISDN 号码真实唯一.该文给出了 MSISDN 号码动态化和虚拟化的核心思想,论证了其可行性,并给出了实现方案.最后通过建立理论模型,对防护机制的防护效能进行了验证和分析.

关键词 通信用户数据;网络空间拟态防御;MSISDN 虚拟化;动态变体

中图法分类号 TP393 **DOI 号** 10.11897/SP.J.1016.2018.00275

A Mimic Defense Mechanism for Mobile Communication User Data Based on MSISDN Virtualization

LIU Cai-Xia JI Xin-Sheng WU Jiang-Xing

(*National Digital Switching System Engineering & Technological R&D Center, Zhengzhou* 450002)

Abstract In this study, we focus on addressing the issue of cellphone user data security in mobile communication networks. The cellphone user data (Hereinafter referred to as user data) contain cellphone users' identification, location identification, routing identification, security parameter set, service profile, and the like. In recent years, facts and studies have shown that these user data are facing serious security problems like being illegally acquired and tampered due to the vulnerabilities in the No. 7 Signaling System (SS7) that is used as one of the fundamental protocols in mobile communication networks. User data, as carriers of user's privacy as well as the fundamental data related to mobile communication, once being illegally acquired or tampered, will lead to user location tracking, fraud, denial of service, or even call interception. Some researchers have mentioned the abusing access way to SS7 networks to acquire or tamper user data, an through the abusing access way we infer that attackers can apply normal SS7 protocol to access core network databases or intercept signaling transmission paths to attack user data, so, conventional passive protection mechanisms powered by anomaly access detections are inadequate.

收稿日期:2016-06-20;在线出版日期:2017-04-08.本课题得到国家自然科学基金创新研究群体项目(61521003)、国家重点研发计划项目课题(2016YFB0800100,2016YFB0800101)和国家留学基金(201407820028)资助.**刘彩霞**,女,1974 年生,博士,研究员,硕士生导师,主要研究领域为无线移动通信技术、信息安全、新型网络体系结构.E-mail:lcxtxr@163.com.**季新生**,男,1968 年生,教授,博士生导师,主要研究领域为无线移动通信技术、信息安全、新型网络体系结构.**邬江兴**,男,1953 年生,中国工程院院士,国内通信与信息技术领域著名专家,主要研究领域包括高性能计算机、宽带信息网、拟态计算与拟态防御.

On the other hand, cellphone user's MSISDN numbers (i. e., cellphone number), which are used as communication identifiers, are normally open to the public, while MSISDN numbers are usually stored and transmitted in mapping state with other data (e. g., IMSI, location identification, subscribed service list, security parameters set), and based on the mapping relationship, almost all the other data items can be retrieved according to MSISDN numbers. Thus, once a cellphone users' MSISDN numbers have been known, it is easy for attackers to access to the user's other data. We infer that user data's mapping-relationship may be a main way that leads to user data leakage. As a result, we dope out a proactive cellphone user data security defense thoughts: to break or conceal the mapping-relationships between users' MSISDN numbers and other data in the insecure SS7 networks. The basic idea of our solution is to establish a Dynamic and Virtual Mapping between cellphone user's MSISDN numbers and other data through adopting dynamic manipulation technique, as such to diversify the mapping relationship. We call this defense mechanism MDM (Mimic Defense Mechanism). The mechanism is characterized by no change in the existing mobile communication network protocol system, and to ensure that one cellphone user's open MSISDN number is the only real. We investigated MSISDN number's attributes, spatiotemporal characteristics, and spatiotemporal mapping-characteristic, demonstrated its feasibility, presented the core idea of MSISDN number dynamics and virtualization, and gave the implementation scheme. In the end, a theoretical analysis model is built to evaluate the MDM's security efficiency. The results show that the proposed MDM mechanism can achieve security improvement without changing the existing network architecture, communication protocol and traffic provision mechanism. In addition, we studied the impacts of multiple parameters (e. g., MSISDN number dynamic-manipulation time interval and the occurrence probability) on security improvement. Such quantitative evaluations offer practical underpinnings of optimizing MDM for other specific application domains.

Keywords cellphone user data; Cyberspace Mimic Defense (CMD); MSISDN virtualization; dynamic manipulation

1 引 言

信息系统的静态性、确定性和相似性为攻击者提供了有利的条件,使其有充足的时间获取实施攻击所需的资源,而且,攻击者一旦获取目标网络或者系统可被利用的资源,可以长时间保持攻击有效.网络空间拟态防御(Cyberspace Mimic Defense,CMD)[1-2]的核心思想就是在功能等价的条件下,以提供目标环境的动态性、非确定性和非持续性为目的,通过动态化、随机化、多样化以及异构冗余等机制方法,实现网络、平台、环境、软件、数据等动态性和不确定性,以扰乱或者瓦解基于确定承载结构上的未知漏洞和后门,从而大幅度增加攻击难度和成本.拟态防御的概念于 2013 年底由邬江兴院士提出,目前被作为一种改变游戏规则的新兴安全技术方向,理论和应用技术已经取得重要成果.

与拟态防御的动态防御思想相似,美国提出了移动目标防御[3](Moving Target Defense,MTD),MTD 的意图也是通过增加系统的不确定性减少系统的可预见性来对抗攻击.目前,业界研究 MTD 的目的主要是解决主机、网络节点设备、应用服务器等通信系统的安全防护问题,防御的主体也是计算机网络典型的攻击手段.

本文主要研究移动通信网中用户数据的安全防护问题.这里的用户数据包括用户的身份标识、位置标识、路由标识、安全参数、业务清单等.这些数据不仅承载着移动通信用户的个人隐私信息,而且作为移动通信的基础数据,广泛分布在移动通信核心网不同网域的设备(如 HLR、HSS、MSC/VLR、SMC、SGSN、CSCF)和信令传递通道中.研究表明,由于移动通信核心网采用的七号信令系统存在安全漏

洞，用户数据很容易通过后门、木马、信令访问以及信道窃听等方式被窃取和破坏. 文献①②③是媒体关于移动通信用户数据被远程获取和攻击的相关事实报道.

通过深入研究移动通信网的架构、协议体系和业务提供模式，我们发现解决用户数据在移动核心网被窃取或被破坏的安全问题，一个有效途径是在移动核心网不可控的通信过程或者通信设备中，隐匿或者打破用户的 MSISDN 号码(Mobile Station International ISDN Number，通常说的手机号码)与同一用户其它数据间的显性关联关系. 因而，本文提出一种移动通信用户数据拟态防御方法. 该方法的核心思想是在保证用户对外公开的 MSISDN 号码真实唯一的前提下，使在网络中传递、存储和使用的 MSISDN 号码具有动态性、多样性和随机性，即在网络中通过对 MSISDN 号码进行动态化和虚拟化改变，有效隐匿用户真实 MSISDN 号码与其它数据在不可控的传递路径和网络设备中的关联关系，从而有效对抗攻击者通过信令过滤、数据库访问、后门、木马或者信令交互等方式获取用户数据的攻击. 本文给出了移动通信用户数据拟态防御的核心思想和实现方案，并基于当前典型的移动通信网络，论证了该机制的可行性和有效性.

本文第 2 节给出相关研究现状；第 3 节给出 MSISDN 号码动态化、虚拟化核心思想，论证其可行性，并给出实现机制；第 4 节分析虚拟 MSISDN 号码资源对拟态防御机制的影响及相关限制条件；第 5 节通过建立理论分析模型，对防护机制的安全效能进行验证和分析；最后一部分是本文小结.

2　相关工作

在移动通信网中，能否对用户身份进行有效认证并且不对无关网络暴露用户身份、位置等隐私信息，一直以来受到业界的广泛关注.

从较早的 GSM 全球移动通信系统至当前最新商用的 LTE 移动通信系统，均在无线接入网采用临时身份标识 TMSI(Temporary International Mobile Subscriber Identity)代替用户的真实身份标识 IMSI (International Mobile Subscriber Identity)，并在无线信道加密，以保护用户身份信息的隐秘性，但对于在特定应用场景仍需在无线信道中明文传递 IMSI 的问题一直未解决. 为此，广大学者投入了大量精力研究移动通信网无线信道 IMSI 的机密性问题④⑤[4,5].

自第三代移动通信系统，国际标准化组织在移动核心网中增加了诸如移动应用部分安全协议(MAPSec)[6]、事务处理能力应用部分安全协议(TCAPSec)[7]、IP 安全协议(IPSec)[8]等网络实体间认证、数据完整性、数据机密性保护等安全机制，一定程度上可以防御假冒、伪装设备对移动核心网的非法访问. 但是，这些安全机制无法抵御用户数据被后门、木马或者通过七号信令被跨网窃取和破坏的安全威胁. 尤其是，上述安全机制(如 MAPSec、TCAPSec)因为实现的复杂性，在现有移动通信网中鲜有部署.

随着移动位置服务(Location Based Service，LBS)的兴起，移动通信网给广大用户或者特定群体提供了方便查询用户位置信息的途径，因而作为用户隐私的位置信息，其安全问题引起业界普遍关注. 目前解决 LBS 业务的位置泄露问题主要有三种技术方法，一种是通过制定常用的隐私管理规则和可信任的隐私协定来约束服务提供商能公平、安全的使用用户 LBS 查询中的位置信息或服务属性[9]；另一种是在 LBS 查询暴露给 LBS 服务器之前，事先对查询中的时空信息或服务属性进行适当地修改或扭曲，使 LBS 服务器无法获得精确的位置信息或服务属性[10,11]；其次是通过使用加密技术使用户的 LBS 查询对 LBS 服务器完全不可见，从而达到隐私保护的目的[12,13]. 文献[14]对上述技术方法的优缺点进行了详细的分析，从中我们可以看出，这些方法都是针对 LBS 业务的应用场景设计的，不适用于移动核心网基于七号信令提供业务的应用场景. 因为，在 LBS 业务场景，使用 LBS 业务的用户需要主动提供自己的位置和服务属性信息给业务服务器，因而，该场景用户隐私泄露的途径是 LBS 业务服务器，防御

① For sale: Systems that can secretly track where cellphone users go around the globe. http://www.washingtonpost.com/business/technology/for-sale-systems-that-cansecretly-track-where-cellphone-users-go-around-the-globe/2014/08/24/f0700e8af003-11e3-bf76-447a5df6411f_story.html, 2014, 08

② Skylock Product Description 2013. http://apps.washingtonpost.com/g/page/busi-ness/skylock-product-description-2013/1276/, 2013, 01

③ SS7: Locate, Track&Manipulate. https://www.youtube.com/watch?v=lQ0I5tl0YLY, 2014, 12

④ Curtis H W. Subscriber authentication and security in digital cellular networks and under the mobile internet protocol. http://citeseerx.ist.psu.edu/viewdoc/down load?doi=10.1.1.24.7355&rep=rep1&type=pdf, 2001

⑤ Arapinis M, Mancini L I, Ritter E. Privacy through pseudonym-mity in mobile telephony systems. http://staging.www.isocdev.org/sites/default/files/05_2_1.pdf, 2014

的核心是解决用户信息提供过程中的防泄露问题.在基于七号信令提供业务的应用场景,由于用户具有全移动网的漫游能力,在用户漫游过程中,用户数据会在移动核心网中广泛传递和使用,用户的身份、位置等敏感信息泄露的重要途径是攻击者利用后门、木马或者信令访问的方式主动获取,因此,在该场景,用户数据防御的核心是解决用户信息在静态存储、动态传递和使用过程中的隐藏问题.

此外,随着移动互联网的快速发展,五花八门的移动应用服务带来的用户隐私信息泄露成为当前业界关注的焦点[15-21].由于部分移动应用服务伴随提供 LBS 业务,如移动在线社会网络,这类应用隐私保护的技术思路与 LBS 业务类似[15].此外,解决其它移动应用服务的隐私泄露问题当前还主要集中在智能终端漏洞发现和漏洞修补方面,如基于安卓移动终端平台开展移动应用服务隐私保护技术的研究[16-17].对于新出现的移动应用服务,对于隐私问题的保护尚处于风险分析评估阶段[18-21].

针对基于移动核心网七号信令系统窃取或者破坏移动通信用户数据的攻击行为,自 2014 年媒体报道了七号信令系统存在安全漏洞之后,业界陆续有解决方案提出①②③④.目前,几乎所有解决方案的基本思路都是在运营商信令网的边界部署信令防火墙,过滤和拦截来自其它运营商网络的异常信令.该方案虽然可以防御来自外部运营商网络的异常信令攻击,但属于被动防护机制,无法解决后门、木马以及基于正常信令的移动通信用户数据窃取和攻击行为.因为攻击者利用后门、木马等手段进行的用户数据窃取和破坏行为,在信令层面可能不会反应出异常.

本文的核心是基于用户 MSISDN 号码动态化和虚拟化机制,研究移动通信核心网中用户数据的主动防护机制,该机制可以有效对抗攻击者利用后门、木马或者信令交互等方式窃取用户数据的攻击,可以有效解决当前七号信令网面临的用户信息安全问题.

3 基于MSISDN虚拟化的拟态防御方法

对移动通信用户而言,因作为其通信标识的 MSISDN 号码对外公开,而在移动通信过程和用户数据存储环节,用户的 MSISDN 与其私有身份标识 IMSI、位置标识、签约业务清单、安全参数等数据项的全部或者部分在网络中显性、直接关联,因而,知道用户的 MSISDN 号码,就可以从用户数据的存储、传输、使用以及管理途径中获取与其关联的其它数据项.这也是当前用户信息在移动通信网泄露或者被恶意窃取和破坏的重要途径.

因而,解决用户数据在移动通信网中的安全问题,一个有效途径是在移动通信网不可控的通信过程或者通信设备中,打破或者隐匿用户的 MSISDN 号码与同一用户其它数据项间的显性关联关系.

3.1 核心思想

基于 MSISDN 虚拟化实现移动通信用户数据拟态防御的核心思想是在试图不影响终端和网络正常业务的前提下,通过动态引入虚拟 MSISDN 号码,建立虚拟 MSISDN 与用户其它数据项间的动态关联,有效打破或者隐匿用户真实 MSISDN 号码与其它数据在不可控的传递路径和网络设备中的关联关系,从而有效对抗攻击者通过信令过滤、数据库访问等途径获取用户数据的攻击.

如果用 ID 表示用户的 MSISDN 号码,用 S 表示用户的其它数据集合,即 $S=\{d_1,d_2,d_3,\cdots,d_k\}$,$d_i$ 表示数据集合中的某类数据,k 表示数据集合中的用户数据种类.则通过在不可控的通信过程或者通信设备中隐匿或者打破 ID 与 S 或者 ID 与 S 的某个子集间的关联关系,就可以大大增加攻击者对用户数据的攻击难度,而对公众移动通信网而言,所有通信设备或者通信过程都可认为是不可控的.可以想象,如果这种关联关系可以动态改变,攻击难度将会进一步增加.

因而,本文实现移动通信用户数据拟态防御的核心思想就是在不可控的通信过程或者通信设备中建立 ID 与 S 或者 ID 与 S 的某个子集间的"动态虚拟关联".具体实现方法就是引入虚拟 MSISDN 号码,对用户在网络中存储和传递的 MSISDN 号码进行动态变体.

具体地,如果用 ID_A 表示用户 A 的 MSISDN 号码,用 S_A 表示用户 A 的其它数据集合,则对用户 A 的数据进行拟态防御,就是在不影响通信和网络业

① Hassan Mourad. The fall of SS7-how can the critical security controls help? https://www.sans.org/reading-room/whitepapers/critical/fall-ss7-critical-security-controls-help-36225, 2015

② Adaptive mobile SS7 protection: Securing the network against privacy & fraud attacks. http://www.adaptivemobile.com, 2014, 12

③ Signaling network vulnerabilities exposed: Protection strategies for operators: http://ww w.xura.com, 2015, 11

④ P1 Security. SS7 Map. http://ss7map.p1sec.com P1, 2014, 12

务的前提下，定期或不定期地为用户 A 分配虚拟的 MSISDN 号码，以在用户数据的存储和传递路径上，隐藏用户真实 MSISDN 号码与其它用户数据间关联关系，如图 1 所示.

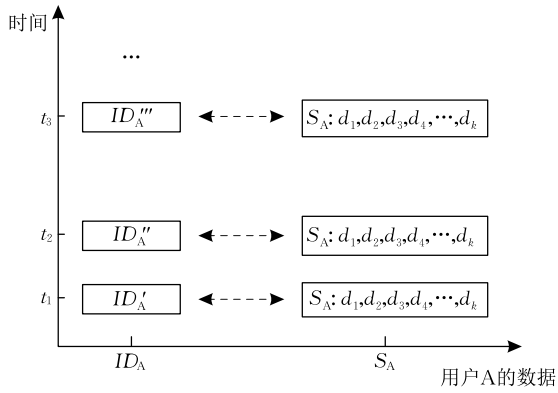


图 1　用户的 MSISDN 号码与该用户其它数据项间的动态虚拟关联关系

图 1 中，t_1、t_2 和 t_3 表示系统对用户 A 的 MSISDN 号码实施动态变体的时间点，ID_A'、ID_A''、ID_A''' 表示在不同的时间点，系统为用户 A 分配的虚拟 MSISDN 号码的取值，每个虚拟号码的有效期从该号码的分配时刻开始，到下一个新号码的分配时刻结束.

基于上述思想，我们需要进一步解决的关键问题是：在当前的移动通信机制下，用户 MSISDN 号码的取值能否动态变体以及怎样实现动态变体.

3.2　MSISDN 号码动态变体的可行性分析

基于典型制式移动通信网的协议体系和业务提供模式，我们对移动通信用户相关数据的属性、时空特性以及时空关联特性进行了深入剖析，并给出了用户数据在移动通信网中可以被动态改变的条件和场景，即那些在网络协议体系中具备“动态变更身份”的用户数据，当满足“非本地产生”，并且“处于非主导角色”两个条件时，可以对其动态改变.

所谓具备“动态变更身份”是指在现有移动通信网的协议体系中，用户终端设备或者网络可以通过标准的通信流程对该数据进行修改. 所谓“非本地产生”是指在用户数据的“时空关系谱”序列中，该用户数据不是当前网元（在移动通信网中，网元是对网络设备的一种称呼）产生的. 所谓处于“非主导角色”，是指在特定的应用场景，某用户数据在通信过程中起辅助作用，如号码显示、计费等. 这里，移动通信的特定场景用时间域描述，特定网元用空间域描述.

基于上述研究，我们进一步分析了 MSISDN 号码的属性（用 A 表示）以及在不同时空中具有的功能（用 F 表示）、角色（用 R 表示）及关联关系，后三类我们统称之为 MSISDN 号码的“时空特性”.

其中，MSISDN 号码的“属性”包括其定义、结构、来源等. MSISDN 号码的“功能”根据移动通信场景，可能是路由寻址功能、计费功能、号码显示功能等. 在特定时空中的“角色”用主导（M）、辅助（A）和可选（O）描述. 这里的关联关系是指在特定场景和特定网元中，与 MSISDN 号码直接关联的用户数据的列表. 移动通信机制决定，当 MSISDN 号码在某个特定时空中处于主导角色时，该数据是不能改变的.

图 2 标示了用户的 MSISDN 号码在特定场景、特定网元中的属性和时空特性. 其中属性、功能、角色在图 2 中分别用 A、F、R 表示，关联关系在图 2 中用 $(d_i,d_j,\cdots)$ 表示. 在不同的时空坐标中，A、F、R 以及 d_i、d_j 等的取值可能是不同的.

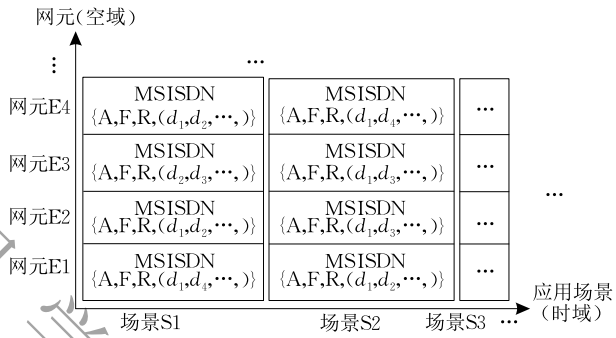


图 2　MSISDN 号码的属性和时空特性

对 MSISDN 号码的属性及时空特性的分析是我们研究 MSISDN 号码是否可以动态变体以及如何实现动态变体的基础.

基于上述对 MSISDN 号码属性和时空特性的研究，结合现有移动通信机制和不同体制网络的协议体系及业务提供模式，我们对 MSISDN 号码是否可以动态变体进行了定性分析，从如下四个方面说明了其可行性.

首先，MSISDN 号码的来源和现有移动通信业务提供机制确定了其具备“动态变更”资质. MSISDN 号码由用户的归属网络运营商分配，用户开户时，先前存储于归属位置寄存器 HLR（Home Location Register）中的某个 MSISDN 号码与用户签约数据关联，这些签约数据包括 IMSI、业务清单、安全参数等，因而，用户 MSISDN 号码的变更过程本质上是用户签约数据与当前 MSISDN 号码解除关联、与新 MSISDN 号码建立关联的过程.

其次，移动通信协议提供了支持 MSISDN 号码变更的协议流程. 当一个新的 MSISDN 号码在 HLR

中与某用户的签约数据关联后，HLR 利用网络提供的协议流程通知其它相关网络实体对该用户的 MSISDN 号码进行实时更新，以保证后续的移动通信业务正常进行. 具体地，不同制式网络的协议流程可分别参见 3GPP 的标准 TS29.002[22] 和 ANSI 的标准 TIA-EIA-41D[23].

再其次，MSISDN 号码由用户归属网络分配的特点使得对其进行动态变体具有很好的可控性. 这种可控性体现在三个方面，第一，单点操作，可控性强，第二，实施动态变体的时机和条件易控，第三，统筹调整和分配虚拟 MSISDN 资源可控.

最后，移动通信流程决定移动终端不需要存储用户的 MSISDN 号码，因而 MSISDN 在网络中被虚拟化后，不需要考虑和终端的一致性问题. 因此对 MSISDN 进行动态变体，不需要修改现有通信协议，可以做到安全机制实施带来的影响最小.

3.3 MSISDN 号码动态变体实现方案

我们在设计用户数据防护机制和实现方案时，除了考虑防护效果外，还以尽可能减小防护机制对现有网络和用户的影响为原则. 因而，基于 MSISDN 虚拟化的拟态防御机制满足三个目标.

第一，MSISDN 虚拟化机制对终端用户是透明的，也就是说，该机制要保证作为用户对外公开的 MSISDN 号码真实唯一，而且保持不变.

第二，该机制不改变现有网络的协议体系和业务提供模式.

第三，该机制要保证每次为用户分配的虚拟 MSISDN 号码不可预测，且同一用户 MSISDN 号码的变换频率能够最大限度地抵御攻击者对新信息的探查能力.

本部分，通过分析不同应用场景 MSISDN 号码在网络中的传递机制，引出 MSISDN 号码动态变体的实现思路.

图 3 示例了移动通信网中用户（以用户 A 为例）MSISDN 号码的传递方向. 其中，号码的归属 HLR 是其最初的存储地，也就是说，当一个用户在移动通信网中开户时，其 MSISDN 号码是存储于某个 HLR 中的（如 HLR_A），随着用户终端开机和在网络中注册，其 MSISDN 号码从 HLR 传递给当前为用户服务的 MSC/VLR 实体（如 MSC_A/VLR_A）. 服务 MSC/VLR 实体在用户的后续业务执行过程中，会将该号码传递给其它网络实体（如图中的 MSC_B/VLR_B、SMC），完成号码显示、计费等功能. 另一方面，当其它用户（如用户 B）与用户 A 通信时，用户 A 的 MSISDN 号码将作为用户 A 的身份标识和路由标识，从用户 B 的终端设备传递到网络. 由于从移动终端 B 到网络的传递路径上，用户 A 的 MSISDN 号码与用户 B 的数据项不存在关联关系，所以传递过程中保留用户 A 的真实 MSISDN 号码不会引起用户 A 其它数据项的泄露.

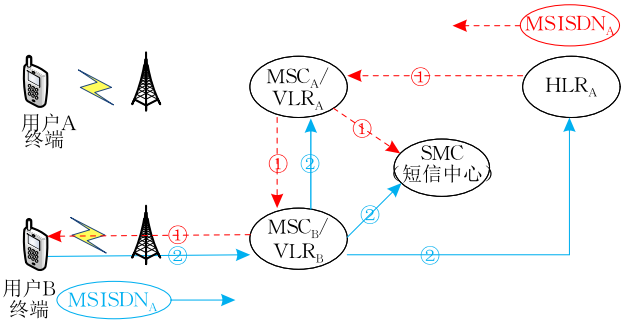


图 3 MSISDN 号码在网络中的传递方向

考虑本文拟态防御机制设定的目标，基于 MSISDN 号码在网络中的传递机制，我们设计了 MSISDN 号码的动态变体实现方案.

方案包括三部分，分别是功能实现方案、部署方案和资源配置管理方案. 本小节简要介绍实现方案和部署方案，资源配置管理方案在第四部分介绍.

MSISDN 号码动态变体由三类功能模块完成. (1) 虚拟 MSISDN 号码分配管理模块；(2) 动态变体规则配置模块；(3) 虚拟 MSISDN 号码与真实 MSISDN 替换处理模块.

虚拟 MSISDN 号码分配管理模块负责管理 MSISDN 资源池，在规则配置模块的控制下，识别特定的应用场景，为本 HLR 归属用户分配 MSISDN “变体”，并保存“变体”与“原体”（原体是指用户的真实 MSISDN 号码）的关联关系，同时基于标准的通信流程，将当前产生的变体传递给特定的网元.

动态变体规则配置模块根据用户安全等级配置动态变体策略、设置动态变体触发条件和变体频率等. 如动态变体触发模式可以有三种，一种是事件触发模式，当识别出与用户数据安全相关的异常事件时，触发 MSISDN 动态变体；一种是周期触发模式，设定 MSISDN 动态变体的时间周期，定期触发 MSISDN 动态变体；第三种是事件触发和周期触发绑定使用. MSISDN 动态变体概率和频率可以根据用户等级设定不同的值，用户安全等级高，变体概率和变体频率设定相对高的值，否则，设定相对低的值.

虚拟 MSISDN 号码与真实 MSISDN 号码替换处理模块根据特定场景的移动通信流程需要，完成用户虚拟 MSISDN 号码到真实 MSISDN 号码的转

换，或者完成真实 MSISDN 号码到虚拟 MSISDN 号码的转换. 前者的操作在 MSISDN 号码从网络向终端传递的过程完成，目的是确保虚拟号码对终端用户的无感存在；后者的操作在 MSISDN 号码从终端传递给网络后完成，目的是确保 MSISDN 号码在网络中传递、存储和使用的隐蔽性.

由上述功能描述，我们可以看出本方案设计的三个功能模块之间存在较清晰的逻辑关系，而每个模块的功能独立于现有任何网络功能实体，与网络实体间不存在信令接口，只是透明串接在相关功能实体的相关对外接口上，因而该方案不会改变当前移动通信系统的网络架构和协议体系. 此外，由三类功能模块的功能我们看出，该方案的实施有三个环节：(1) 配置一定数量的 MSISDN 号码资源；(2) 在特定的事件发生时或者周期性地为特定用户分配虚拟 MSISDN 号码；(3) 在特定的用户通信场景，按需实现真实 MSISDN 号码与虚拟 MSISDN 号码的替换. 因此，该方案逻辑关系简单，在现有网络架构下易于实现. 基于图 3，我们给出了三类功能模块的逻辑关系及在网络中的部署示意，参见图 4.

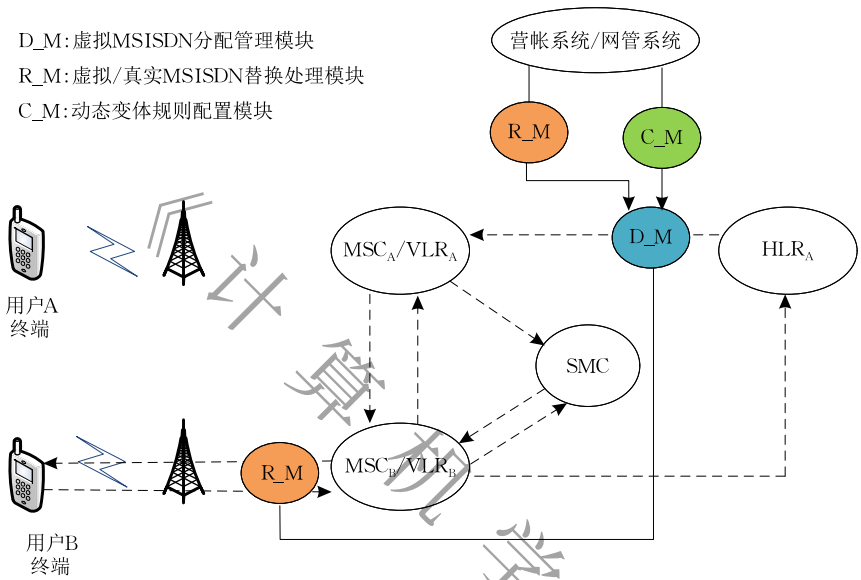


图 4　MSISDN 动态变体功能模块间的逻辑关系及部署示意图

为验证基于 MSISDN 虚拟化实现移动通信用户数据拟态防御机制的可行性，基于上述方案，作者所在的研究团队研制了基于 MSISDN 虚拟化的拟态防御原理样机. 在原理样机中，采用了两种虚拟 MSISDN 号码的动态分配策略，一种是由用户移动性管理事件触发，另一种是周期触发. 根据通信需要，虚拟 MSISDN 号码和真实 MSISDN 号码的替换只发生在用户发起呼叫(或短信)或者被呼叫(或接收短信)的场景. 由于单用户的移动性管理事件和呼叫事件的平均发生率通常以小时计，因而 MSISDN 虚拟化机制对移动通信系统的处理能力影响可以忽略不计. 实验也验证了本文的机制对网络和系统的处理开销基本无影响. 由于篇幅所限，本文省略了相关内容.

下面，我们分析为确保拟态防御机制有效，虚拟 MSISDN 资源的配置问题.

4　虚拟 MSISDN 资源配置

不难看出，基于 MSISDN 虚拟化的移动通信用户数据拟态防御机制的防护效果与虚拟 MSISDN 号码的资源配置有直接关系，也就是说，要实现我们的防护目标，需要有足够的 MSISDN 号码资源作保证，并且 MSISDN 号码的数量与系统防护的用户数量及虚拟 MSISDN 号码的变换频率有密切关系. 下面我们给出理论分析方法，以此为工程实施提供参考和依据.

MSISDN 号码作为运营商的规划数据，与 IP 地址类似，不仅有严格的结构和编码，而且因其具有路由寻址功能，所以运营商给不同归属网络分配的 MSISDN 号段有明确限制，也就是说，分配给一个归属网络的号段，不能同时分配给其它归属网络.

要实现拟态防御目标，待分配的虚拟 MSISDN 号码资源要满足如下两个条件：

(1) 同一个虚拟 MSISDN 号码不能同时分配给两个用户，且一个虚拟 MSISDN 号码在某个分配时间间隔 T 内，不能被重复分配两次；

(2) 分配给同一个归属网络的 MSISDN 号码资

源要满足虚拟 MSISDN 号码分配的视在随机性，也就是说，为某个归属网络分配的虚拟 MSISDN 资源应该与此归属网络对虚拟 MSISDN 资源的需求相一致.

因为不同归属网络有不同数量的号段需求，运营商可供分配的号段大小可能也不一样，如大多数号段是四位数字，有的号段可能是 3 位数字，号段大小不同意味着可供分配的 MSISDN 号码数量不同，我们试着采用可满足模理论[24](Satisfiability Modulo Theories，SMT)来分析该问题.

我们先做如下假设和定义.

(1)假设一个运营商网络有 m 个需要实施防护的用户，用 U 表示需要实施防护的用户集合，则 $U=\{U_1,U_2,\cdots,U_m\}$.

(2)假设有 L 个归属网络，归属网络的集合用 N 表示，$N=\{N_1,N_2,\cdots,N_L\}$，则每个需要防护的用户 U_i 都归属于集合 N 中的一个特定的网络 N_j. 假设每个归属网络都配置 1 个 HLR 管理归属于本网络的用户数据，且 HLR 的容量足够大.

(3)假设共有 n 个空闲的 MSISDN 号段可供虚拟 MSISDN 分配，分别记为号段 $S_1,S_2,\cdots,S_n$，用 $|S_k|(k=1,2,\cdots,n)$表示每个号段可分配的 MSISDN 号码数量.

(4)根据用户的安全等级，为用户设定最小的虚拟 MSISDN 变化频率，通常，越是敏感用户，为其分配虚拟 MSISDN 号码的频率应该越高，假设用户 U_i 的虚拟 MSISDN 最小变化频率为 R_i.

(5)定义布尔变量 $b_{kj}\in[0,1]$，用于标识空闲号段 S_k 是否分配给归属网络 N_j，当号段 S_k 分配给子网 N_j，$b_{kj}=1$，否则取值为 0. 因为同一个 MSISDN 号段只能分配给一个归属网络，所以 b_{kj} 要满足式(1)

$$\sum_{j=1}^{L} b_{kj}=1,\ k=1,2,\cdots,n \tag{1}$$

式(1)可以看作是MSISDN号段分配的限制条件.

(6)定义布尔值 c_{ij}，用于指示用户 U_i 属于归属网络 N_j.

(7)定义时间变量 T，用于指示同一个虚拟 MSISDN 号码不能被重复分配两次的间隔.

由上，在时间间隔 T 内，系统要为任意用户 U_i 至少提供 $R_i\times T$ 个虚拟 MSISDN 号码资源，因此，要为 m 个用户的数据提供拟态防御，系统至少需要提供式(2)所示的 MSISDN 号码资源.

$$N_{\mathrm{MSISDN}}=\sum_{i=1}^{m} R_i\times T \tag{2}$$

而为用户分配虚拟 MSISDN 的频率 R_i 要满足式(3)所示的限制条件.

$$\left(\sum_{i=1}^{m} c_{ij}R_i\right)\times T\le\sum_{k=1}^{n} b_{kj}|s_k|,\ j=1,2,\cdots,L \tag{3}$$

此外，由于为每个归属网络分配的 MSISDN 号码资源至少满足每个归属网络所有防护用户所需的虚拟 MSISDN 资源总数. 为此，我们再定义两个变量：

(1)单个归属网络的需求分配比 W_j：定义为归属网络 N_j 中的防护用户需要虚拟 MSISDN 号码资源的数量与实际分配给该归属网络的号码资源的比值，则 W_j 可以用式(4)表示.

$$W_j=\frac{\left(\sum_{i=1}^{m} c_{ij}R_i\right)\times T}{\sum_{k=1}^{n} b_{kj}|s_k|},\ j=1,2,\cdots,L \tag{4}$$

由式(3)，$W_j\le 1$.

(2)整个网络的需求分配比 W_a 定义为一个运营商网络所有防护用户所需虚拟 MSISDN 资源的数量与网络中空闲 MSISDN 号码数量的比值. 则 W_a 可以用式(5)表示.

$$W_a=\frac{\sum_{i=1}^{m} R_i\times T}{\sum_{k=1}^{n}|s_k|} \tag{5}$$

要满足 MSISDN 号码资源分配的相对合理性，单个网络的需求分配比要与整个网络的需求分配比基本相当. 因而，W_j 和 W_a 的关系可以用式(6)表示.

$$W_j\ge W_a,\ j=1,2,\cdots,L \tag{6}$$

为便于用 SMT 解算器求解，把式(6)用式(7)表示.

$$|W_j-W_a|<\sigma,\ j=1,2,\cdots,L \tag{7}$$

其中 σ 是一个常量.

根据式(1)、式(3)和式(7)的限制条件，可以采用 SMT 解算器[15]来求解，寻找 b_{kj} 的取值. 在求解过程中，可以先设置一个 T 的初值，如 $T=\sum_{k=1}^{n}|s_k|\Big/\sum_{i=1}^{m}R_i$，$\sigma$ 设置一个默认值，如取 0.1，并断言限制条件. 如果没有得到有效解，我们减少 T 的取值，增大 σ 的取值，再断言限制条件，重复上述过程，直到找到一个有效解.

以上是虚拟 MSISDN 号码资源分配问题的分析和求解方法.

此外，由式(2)，我们可以得出归属网络虚拟

MSISDN 号码资源的配置需求与需要防护的用户数量(m)以及与虚拟 MSISDN 分配间隔($1/R_i$)间的关系，如图 5 所示. 这里假设每个用户的虚拟 MSISDN 号码的最低分配频率相同.

图 5 所示结果，可以作为移动通信用户数据拟态防御机制工程实现的参考.

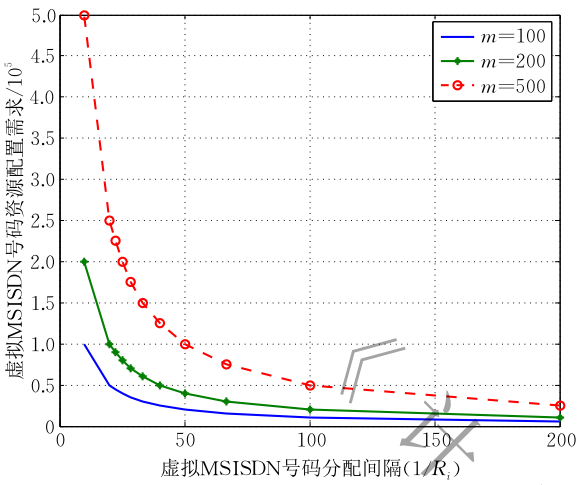


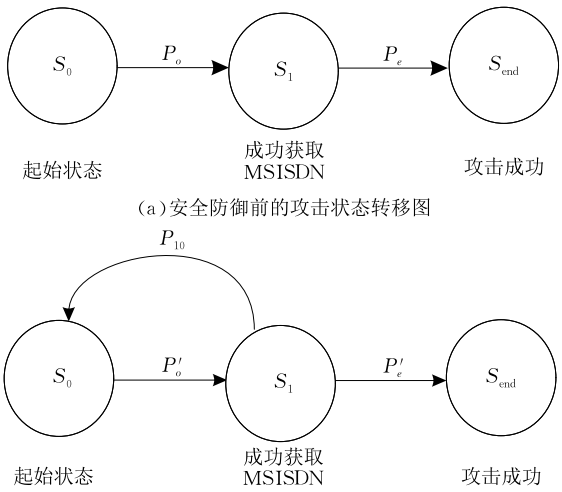
图 5　虚拟 MSISDN 资源配置需求与虚拟 MSISDN 分配间隔及防护用户数量的关系

5　防护效能分析

由前面的分析，攻击者一旦获取用户的 MSISDN 号码，就可能通过信令过滤或者数据库访问等方式，获取与 MSISDN 号码关联的用户其它数据. 通过引入虚拟 MSISDN 号码机制，可以使攻击者之前获取的用户 MSISDN 号码无效，因而，要实现对用户数据的攻击，必须重新获取. 我们可以想象，当用户虚拟 MSISDN 号码的分配间隔小于攻击者重新获取目标用户 MSISDN 号码和基于新的 MSISDN 号码获取用户数据所花费的时间时，将达到非常好的用户数据防护效果.

本部分将分析虚拟 MSISDN 号码分配的相关参数对拟态防御机制防护效能的影响.

我们分别用图 6(a)和(b)描述系统引入拟态防御机制之前和之后，攻击者的攻击状态转移过程. 假设攻击者尝试获取一个 MSISDN 号码失败或者在基于已知的 MSISDN 号码尝试获取该号码关联的其它数据时失败，就结束对该用户的攻击尝试；而如果攻击者在获取用户数据的过程中，发现已获取的 MSISDN 发生变化，则会尝试重新获取. 这个假设符合一般攻击者的心理.



(a)安全防御前的攻击状态转移图

(b) 安全防御后的攻击状态转移图

图 6　攻击者的攻击状态转移图

用 P_o、P'_o分别表示引入安全防御机制前、后攻击者由初始状态(S_0)获取用户 MSISDN 的成功概率(S_0状态到 S_1状态的转移概率). 用 P_e 和 P'_e分别表示引入安全防御机制之前和之后攻击者基于 MSISDN 成功获取用户其它数据的概率(S_1状态到 S_{end}状态的转移概率). P_{10}表示攻击者已经获取一个用户的 MSISDN(或者虚拟 MSISDN)号码后，该用户的 MSISDN 号码(或虚拟号码)发生变体的概率，也就是 S_1状态到 S_0状态的转移概率.

如果用 P_{succ} 和 P'_{succ}分别表示引入安全防御机制之前和之后攻击者攻击成功的概率，则 P_{succ} 和 P'_{succ}可以分别用式(8)和式(9)表示.

$$P_{succ}=P_o\times P_e \tag{8}$$

$$P'_{succ}=P_{S_1}\times P'_e \tag{9}$$

其中，P_{S_1}表示系统引入拟态防御机制后，攻击者处于状态 S_1的稳态概率.

下面，我们在第四部分相关假设和定义基础上，新定义几个参量.

(1)攻击者获取用户 MSISDN 号码的时间间隔(T_r). 攻击者获取一个用户的 MSISDN 号码所需平均花费的时间，攻击者获取用户 MSISDN 号码的途径有很多，假设其每次获取同一个用户的 MSISDN 号码花费的时间相同；

(2)用户 MSISDN 动态变体时间间隔(T_d). 系统对用户的 MSISDN 号码实施动态变体的平均时间间隔. 在某个动态变体的时间间隔内，系统是否给某个用户分配新的虚拟 MSISDN 号码，由当前的场景以及防护策略决定，假设在一个动态变体间隔内，系统以概率 P_u给用户分配新的虚拟 MSISDN 号码.

(3)攻击者获取用户其它数据的时间间隔(T_e).攻击者获取用户的 MSISDN 号码后,基于 MSISDN 号码获取其它用户数据平均需要花费的时间.攻击者基于 MSISDN 号码获取其它用户数据的途径有多条,假设不同途径平均用时相同.

可以分析,当攻击者由初始状态 S_0 获取一个用户的 MSISDN 后,进入 S_1 状态,在试图获取用户其它数据的过程中(在 T_e 时间段内),如果系统对该用户的 MSISDN 行了动态变体,则攻击者已经获取的 MSISDN 值无效,故转入初始状态 S_0,重新获取 MSISDN.

下面我们分析 P_{10}、P'_o、P_{S_1} 以及 P'_e的取值.

转移概率 P_{10} 表示当攻击者处于 S_1 状态时,MSISDN 发生变体的概率.由于在任一个动态变体时间间隔 T_d 时间内,一个用户的 MSISDN 发生变体的概率是 P_u,因而不发生变体的概率是 $1-P_u$.在攻击者获取用户数据的任一时间间隔 T_e 内,将有 T_e/T_d 次变体发生,所以在假设当前变体事件与前面的变体事件不相关时,在 T_e 时间间隔,该用户的 MSISDN 未发生变体的概率是 $(1-P_u)^{T_e/T_d}$,发生变体的概率为 $1-(1-P_u)^{T_e/T_d}$.所以,

$$P_{10}=1-(1-P_u)^{T_e/T_d} \tag{10}$$

P'_o 表示系统采用拟态防御机制后,攻击者在 T_r 时间段内成功获取一个用户的 MSISDN 的概率,则 P'_o 可以用下式表示.

$$\begin{aligned}P'_o=&\{T_r\text{时间段内,成功获取 MSISDN,}\\&\text{且 MSISDN 未发生变体}\}\\=&P_o\times(1-P_u)^{T_r/T_d}\end{aligned} \tag{11}$$

同理,P'_e 可以用式(12)表示.

$$\begin{aligned}P'_e=&\{T_e\text{时间段内,成功获取用户其它数据,}\\&\text{且 MSISDN 未发生变体}\}\\=&P_e\times(1-P_u)^{T_e/T_d}\end{aligned} \tag{12}$$

我们可以分析,图 6(b)所示的攻击过程在 t 时刻的状态只与前一时刻的状态有关,与之前的状态无关,所以,可以把图 6(b)所示的攻击状态转移过程看成是一个简单的马尔科夫过程,而 P_{10}、P'_o 和 P'_e 是状态转移概率.得到 P_{10}、P'_o、和 P'_e,根据马尔科夫链特性,我们就可以求解每个状态的稳态分布,然后根据式(9)可以求解 P'_{succ}.

再定义 γ 为系统实施拟态防御机制后,用户数据攻击难度的增量,用攻击成功率下降的倍数表示,所以 γ 可用式(13)表示.

$$\gamma=\frac{P_{\text{succ}}}{P'_{\text{succ}}}-1 \tag{13}$$

首先分析 MSISDN 动态变体时间间隔 T_d 对防护效果的影响.

设定攻击者获取 MSISDN 平均花费的时间 T_r 和基于 MSISDN 获取其它数据平均花费的时间 T_e 取固定值 50 和 60,P_u、P_o、P_e 分别取 0.7、0.8、0.8,分析当 T_d 分别取 60、70、80、90、100、110、150、200、500、100000(近乎静态)时,攻击者对移动通信用户数据的攻击成功率及攻击难度的增量.表 1 标示了攻击成功率和攻击难度增量随 T_d 取值的变化情况.

表 1 攻击成功率和攻击难度增量随 T_d 取值的变化($T_r=50$,$T_e=60$)

T_d	P'_{succ}	γ
60	0.0604	9.595
70	0.0805	6.947
80	0.0995	5.435
90	0.1168	4.479
100	0.1325	3.830
110	0.1466	3.365
150	0.1901	2.367
200	0.2250	1.845
500	0.2969	1.156
100000	0.3492	0.833

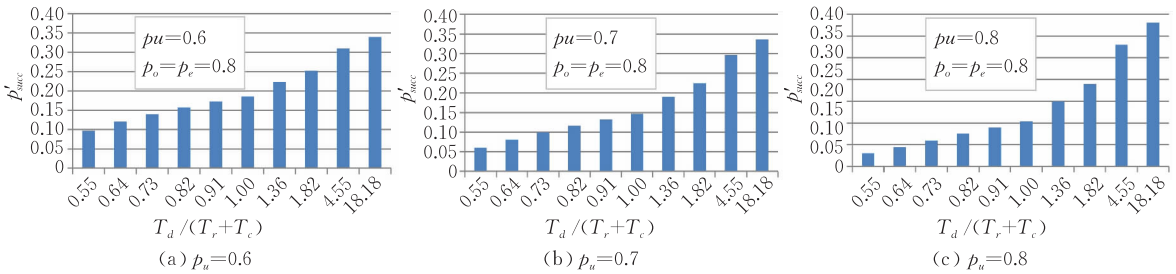
图 7 和图 8 比较直观地展示了拟态防御效果与虚拟 MSISDN 变化频率的关系.其中图 7 示意了采用拟态防御机制后,攻击者的攻击成功率(P'_{succ})随 $T_d/(T_r+T_e)$ 的变化情况;图 8 示意了采用拟态防御机制后,攻击者的攻击难度增量(γ)随 $T_d/(T_r+T_e)$ 的变化情况.

由表 1、图 7 和图 8 可以看出,当 $T_d<(T_r+T_e)$ 时,攻击成功率很低,攻击难度增加比较明显,这与实际情况吻合.也就是说,当虚拟 MSISDN 的平均变化时间间隔小于攻击者获取 MSISDN 和基于 MSISDN 获取用户其它数据花费的平均时间时,防护效果明显.

实际工程实施时,T_d 并不是取越小越好,还需考虑动态变体对系统资源的占用情况,这也是作者后续工作研究的重点.

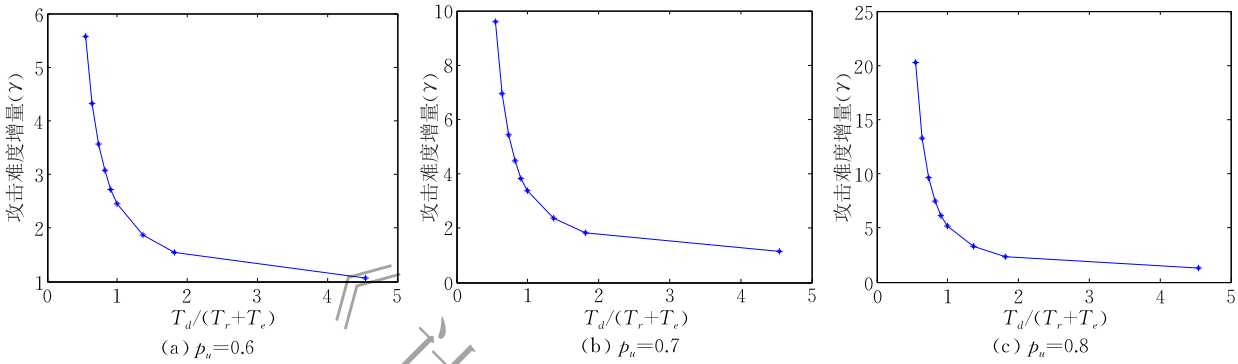
此外,我们再分析虚拟 MSISDN 动态变体概率对防护效果的影响.我们设定 P_o 和 P_e 分别取 0.7 和 0.8,$T_r=50$,$T_e=60$.图 9(a)和图 9(b)分别示意了当 MSISDN 分别以不同概率动态变体时,攻击者的攻击成功率和攻击难度增量随 $T_d/(T_r+T_e)$ 变化的情况.从图 9(a)可以看出,采用拟态防御机制后,攻击者的攻击成功率随着 MSISDN 的动态变体概率的增大而降低;从图 9(b)可以看出,采用拟态防御机制后,攻击者的攻击难度增量随着 MSISDN 的动态变体概率的增大而增大,并且增加幅值比较明显.

上述结果有助于更直观地配置防护规则.



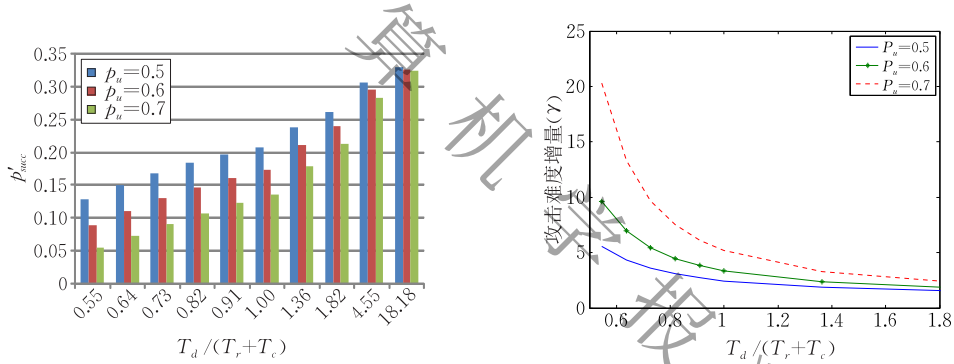
(a) p_u=0.6　(b) p_u=0.7　(c) p_u=0.8

图 7　攻击成功率随 $T_d/(T_r+T_e)$的变化趋势



(a) p_u=0.6　(b) p_u=0.7　(c) p_u=0.8

图 8　攻击难度增量随 $T_d/(T_r+T_e)$的变化趋势



(a) 攻击成功率随MSISDN动态变体概率的变化情况　(b) 攻击难度增量随MSISDN动态变体概率的变化情况

图 9　MSISDN 动态变体概率对防护效果的影响

综上分析，我们可以得到如下结论：(1) 本文提出的基于 MSISDN 动态变体实现移动通信用户数据的拟态防御机制可以有效增加攻击者的攻击难度，降低其攻击成功率；(2) 虚拟 MSISDN 动态变体的时间间隔和发生概率对攻击难度或者攻击成功率有显著影响.

6　结束语

基于对移动通信用户数据安全威胁的认识，本文基于拟态防御思想，提出一种基于 MSISDN 虚拟化的移动通信用户数据防护方法，该机制在考虑安全防护效果的同时，不改变现有网络协议体系和业务提供模式，是拟态防御思想在移动通信领域的有效尝试.

本文首先分析了移动通信用户信息泄露和被窃取的首要途径，提出了基于 MSISDN 动态化和虚拟化的拟态安全防护思想，即通过在不可控的通信过程和通信设备中给用户动态分配虚拟的 MSISDN 号码，实现 MSISDN 号码与其它数据间关联关系的多样化. 基于上述防护思想，本文基于典型制式的移动通信网络，剖析了 MSISDN 号码的属性和时空特性(包括在不同应用场景的功能、角色以及在不同时空中的关联特性)，并结合移动通信机制和不同体制网络的协议体系及业务提供模式，对 MSISDN 动态化和虚拟化机制的可行性进行了论证，提出了拟态防御机制的实现方案，并给出了虚拟 MSISDN 号码的资源配置方法. 最后通过建立理论分析模型，对防护机制的有效性进行了验证. 结果表明，在不改变现有移动通信协议和业务提供模式的基础上，本文的

拟态防御机制能够达到很好的用户数据防御效果.此外,论文还分析了动态变体参数对安全防御效果的影响,为工程实现提供了参考和依据.

本文提出的移动通信用户数据防护方法可以为不同应用场景的信息安全或者隐私安全机制提供参考.将拟态防御机制应用于其它应用场景也是作者后续的重要工作之一,此外,作者还将继续研究拟态防御机制对系统性能的影响.

参 考 文 献

[1] Wu Jiang-Xing. Meaning and vision of mimic computing and mimic security defense. Telecommunications Science, 2014, 30(7): 4-9(in Chinese)
(邬江兴. 拟态计算与拟态安全防御的原意和愿景. 电信科学, 2014, 30(7): 4-9)

[2] Wu Jiang-Xing. Research on cyberspace mimic defense. Journal of Cyber Security, 2016, 1(4): 1-10(in Chinese)
(邬江兴. 网络空间拟态防御研究. 信息安全学报, 2016, 1(4): 1-10)

[3] Jajodia S, Ghosh A K, Swarup V, et al. Moving Target Defense: Creating Asymmetric Uncertainty for Cyber Threats. New York, USA: Springer, 2011: 54

[4] Køien G M, Haslestad T. Security aspects of 3G-WLAN interworking. IEEE Communications Magazine, 2003, 41(11): 82-88

[5] Lee Wei-Bin, Yeh Chang-Kuo. A new delegation-based authentication protocol for use in the portable communication systems. IEEE Transactions on Wireless Communications, 2005, 4(1): 57-61

[6] MAP application layer security. 3GPP standard TS 33.200, 2007

[7] Transaction Capabilities Application Part(TCAP) user security. 3GPP standard TS33.204, 2006

[8] Perlman R, Kaufman C. Analysis of the IPSec key exchange standard//Proceedings of the 10th IEEE International Workshops on Enabling Technologies Infrastructure for Collaborative Enterprises. Massachusetts, USA, 2001: 150-156

[9] Representation of Uncertainty and Confidence in the Presence Information Data Format Location Object (PIDF-LO). IETF standard RFC 7459, 2015

[10] Dewri R. Local differential perturbations: Location privacy under approximate knowledge attackers. IEEE Transactions on Mobile Computing, 2013, 12(12): 2360-2372

[11] Andrés M E, Bordenabe N E. Geo-indistinguish ability: Differential privacy for location-based system//Proceedings of the 20th ACM Conference on Computer and Communications Security. New York, USA, 2013: 901-914

[12] Gentry C. Fully homomorphic encryption using ideal lattices//Proceedings of the 41st ACM Symposium on Theory of Computing. New York, USA, 2009: 169-178

[13] Yao B, Li F F, Xiao X K. Secure nearest neighbor revisited//Proceedings of the 29th IEEE Internation al Conference on Data Engineering. Piscataway, USA, 2013: 733-744

[14] Zhang Xue-Jun, Gui Xiao-Lin, Wu Zhong-Dong. Privacy preservation for location-based services: A survey. Journal of Software, 2015, 26(9): 2373-2395

[15] Shen N, Yuan K, Yang J, et al. B-mobishare: Privacy-preserving location sharing mechanism in mobile online social networks//Proceedings of the 9th IEEE International Conference on Broadband and Wireless Computing, Communication and Applications. Guangdong, China, 2014: 312-316

[16] Stach C, Mitschang B. Privacy management for mobile platforms—A review of concepts and approaches//Proceedings of the 14th IEEE International Conference on Mobile Data Management. Milan, Italy, 2013: 305-313

[17] Bugiel S, Heuser S, Sadeghi A R. Flexible and fine-grained mandatory access control on android for diverse security and privacy policies//Proceedings of the 22nd USENIX Security Symposium. Washington, USA, 2013: 131-146

[18] Liang X, Zhang K, Shen X, et al. Security and privacy in mobile social networks: Challenges and solutions. IEEE Wireless Communications, 2014, 21(1): 33-41

[19] Zhang K, Liang X, Shen X, et al. Exploiting multimedia services in mobile social networks from security and privacy perspectives. IEEE Communications Magazine, 2014, 52(3): 58-65

[20] Liu B, Lin J, Sadeh N. Reconciling mobile app privacy and usability on smartphones: Could user privacy profiles help?//Proceedings of the 23rd International Conference on World Wide Web. New York, USA, 2014: 201-212

[21] Damiani M L. Location privacy models in mobile applications: Conceptual view and research directions. GeoInformatica, 2014, 18(4): 819-842

[22] Mobile Application Part (MAP) Specification (Release 9). 3GPP TS 29.002 V9.0.0, 2009

[23] Cellular Radio Telecommunications Intersystem Operations. ANSI/TIA/EIA-41-D-1997, 1997

[24] Bjørner N, de Moura L. $Z3^{10}$: Applications, enablers, challenges and directions//Proceedings of the 6th International Workshop on Constraints in Formal Verification Grenoble. France, 2009: 83-98

LIU Cai-Xia, born in 1974, Ph. D., professor, M. S. supervisor. Her research interests include wireless mobile communication technology, information security and novel network architecture.

JI Xin-Sheng, born in 1968, professor, Ph. D. supervisor. His research interests include wireless and mobile communication technology, information security and novel network architecture.

WU Jiang-Xing, born in 1953, member of China Engineering Academy, a famous expert in the field of communication and information technology in China. His current research interests include novel computer architecture, broadband information network, mimic computing and mimic defense.

Background

This study focuses on protecting cellphone user data in mobile communication networks that are critical infrastructures with approximately four billion users in the world. Mobile communication plays an important role in the military, economic, and political spheres. In recent years, the data security of a large number of mobile communication users has become a major concern.

The cellphone user's data (Hereinafter referred to as user data), which are directly related to communication events, contain cellphone users' identification, location identification, routing identification, security parameters set, service profile list, and the like. Facts and studies have shown that these user data are facing serious security problems like being illegally acquired and tampered due to the vulnerabilities in the No. 7 signaling system that is used as one of the fundamental protocols in mobile communication networks.

For cellphone users, their MSISDN numbers (i. e., cell phone number), which are used as communication identifiers, are normally open to the public, while MSISDN numbers are usually stored and transmitted in mapping state with other data (e. g., IMSI, location identification, subscribed service list, security parameters set), and based on the mapping relationship, almost all the other data items can be retrieved according to MSISDN numbers. Thus, once a cellphone users' MSISDN numbers have been known, it is easy for attackers to access to the user's other data. We infer that user data's mapping-relationship may be a main way that leads to user data leakage. This problem motivates us to incorporate the data dynamics and virtualization technology to develop a mobile communication user data mimic defense mechanism. The core idea of this mechanism is to diversify the mapping relationships between MSISDN numbers and other data by introducing virtual MSISDN number in the uncontrollable communication process and network equipment, which can effectively resist the attacker through signaling filtering and database access to access user data. The method is characterized by no change in the existing mobile communication network protocol system, and to ensure that the user's open MSISDN number is the only real. The author gives the core idea of MSISDN number dynamics and virtualization, demonstrates its feasibility, and gives the implementation scheme. Finally, a theoretical analysis model is established to verify and analyze the security efficiency of the security mechanism.

This work was supported by the Funds for Creative Research Groups of China under Grant NSFC-No. 61521003, the National Key Research Program of China under Grant Nos. 2016YFB0800100 and 2016YFB0800101, and the Visiting Scholar Program of China under Grant of China Scholarship Council-201407820028.