电子身份验证漏洞如何监管

现有身份信息管理手段单一 谁来证明“你就是你”

5月16日,有报道显示中国银联通过大数据统计分析,得出个人网络财产安全的“蚁溃之堤”——个人信息泄露是90%电信诈骗案件成因。

这意味着,在网络世界中,别人可以通过证明“他是我”,借由“我”的身份“招摇撞骗”,掳走“我”的财产。在安全专家的语系里,这样的产业链条被称为黑产。亚信安全副总裁陆光明表示,“从产业规模看,2016年底我国网络电子认证市场还不到200亿元,但是黑产的规模已经高达千亿元左右。”

身份信息在黑市上被明码标价

网络可信身份认证该出手了。“《中华人民共和国居民身份证法》确定居民身份证是公民身份管理的可信依据,网络身份验证也需要可信度、权威级相当的可信平台。”中国工程院院士沈昌祥在日前召开的C3安全峰会上表示,网络身份可信验证工作刻不容缓。

“850块钱,就能买到开房记录、列车记录、航班记录等11项个人隐私数据,在身份黑市上,隐私的买卖是被明码标价的,能够用于制作假通缉令等身份证户籍信息,一条只需要10—40元。”中国科学院信息工程研究所副所长荆继武展示了一张明晰的价码账单,仿造一个企业身份信息的“五证”仅需要千元左右。无论对于自然人还是法人来说,我国网络信息保护的形势都非常严峻。

“易获得”是个人电子信息难以规避的“软肋”。安全领域内,八成以上的信息泄露由内部人员所为。“很少有黑客愿意花那么大的代价从外攻破系统获取信息,从内攻破是更便利、更容易的。”陆光明说。

“既然防不胜防,能不能让这些偷窃泄露来的信息分文不值呢?现实生活中身份证的使用对此提供了很好的借鉴。”陆光明说。

如何让网络身份认证与现实身份认证一样“强有力”“无漏洞”,成为一个系统工程,关系到新技术应用、新体系构建、以及与已有法律体系的共享共建。国际上,欧盟2006年出台了开展网络可信身份体系建设的法规。美国2011年公布网络空间可信身份国家战略,提出10年时间建设美国网络身份体系。

网络身份验证难有“防骗”功效

当下使用的网络身份验证难有“防骗”功效,沈昌祥将问题归纳为3类:方法不安全、难保真实性;欠公平公正、难防篡改;缺乏法律效力、难以执法。沈昌祥解释:“例如大量汇集在微信、支付宝上的个人信息,虽然是实名认证,但隶属于第三方企业,难以保障它们的不可更改性、不可复制性。”

陆光明对此持相同观点,他表示,在国外以企业公信力作为社会公信力的商业行为居多,例如谷歌的互联网账号可用作其他跨行业的社会认证。但是,Facebook的身份数据泄露,严重到甚至可能会对美国高层政策施以影响,这一事件令人对这种模式的安全性产生顾虑。

被泄露之外,被利用更使身份信息安全问题“雪上加霜”。陆光明说,韩国2011年就爆发过一次非常严重的身份数据泄露事件,当时有3500万用户数据泄露,占当时韩国网民的95%左右。此事使得韩国政府开始限制网络身份收集,也宣告了其网络实名制的结束。

“身份非法买卖严重影响网络实名制的实施效果。”荆继武说,身份黑市交易可以将个人的网络身份绑定到一个完全不属于本人的现实身份上。

“黑户”的存在,不仅侵害了可能并不知情的个人的利益,也使得真正需要准确掌握身份信息数据的电商深感困扰。“一家电商的责任人表示,他每天有几十万新注册用户,其中有很多黑产用户,电商企业需要花费很多精力、成本去校验新用户,将‘黑户’挑拣出来,确保系统安全。”陆光明说。

荆继武总结道:“现有的身份信息管理技术手段单一、难奏效,需要完备的身份信息数据管理体系。”

搭建有公信力的第三方验证平台

“一些互联网公司开发的APP,注册时需要身份证、姓名、电话等信息。我相信很多人都不愿意透露、被捆绑。”陆光明说,用户很难确定企业是否会将这些信息挪作他用。

通过搭建第三方平台的方法,或能解决这个“隐患”。

陆光明表示,一个保有用户信息的第三方认证平台,可以帮助互联网企业认证用户、也确保用户的信息只用于约定的用途。“对于新型互联网企业来说,平台把认证结果反馈给企业,企业获得的是平台处理过的可信的用户认证。而用户(消费者)需要面对的则是一个有公信力的平台,而不是多个信息不对等的企业。”

先前已经聚集了大量客户信息的淘宝、微信等已经开始担负起这样的角色,目前,已经有“授权认证”等模式,让用户无需再次注册新应用的账号。荆继武表示,背后基于多模式多安全等级的电子认证技术,也保证了“不同等级的数据库使用者,能够接触到的信息是不同的。”

“基于庞大的互联网用户数据基础,亚信安全之前就曾做过类似的平台构建。”陆光明说,随着国家互联网+政务战略部署的提出,亚信安全希望构建一个能够打通政务体系的、拥有法律效力的认证平台。

目前国家层面正在构建具有法律效力的权威性公民网络电子身份标识基础设施,并加快与电子身份应用相关的技术和标准的研制推广工作,未来将会加速构建和网络电子身份基础设施配套的基础服务能力,基于网络电子身份标识基础设施将会出现更多的行业化、跨领域的高可信、互信任的认证平台系统。

陆光明介绍,由国家不同部委授权建设,亚信安全参与搭建统一的身份信息认证平台,不仅仅要完成个人身份认证业务,还提供涉及到法人、营业执照等证照信息的认证服务。纵向来看,整个平台包括国家中心平台的建设,也包括中心平台与各个部委、各省市的对接建设。

为了担负起庞大的信息处理量,平台将构建分布式的数据存储,并推动数据共享,打破数据孤岛,推进电子签名应用等,以期形成跨行业的身份信息认证的传递和互认。通过推动单纬度、单系统、特定场景的可信身份,向多维度、综合性、可交叉的可信身份体系,助力网络安全身份体系发展。

相关链接

新技术让网上身份识别更可靠

居民身份证作为电子法定证件,本身兼有“线下”和“线上”法律作证的地位。沈昌祥表示,2代身份证识别体系建设时,预留了指纹识别的端口,当时由于种种原因暂时未被整合的认证手段,最近可能再被启用。

“公民网络电子身份标识基础设施将融合各种新技术。”陆光明说,企业将持续创新可交互、易操作、高可信的新型认证技术,例如声纹识别、指纹识别、相貌识别等。

之前的身份可信判断,通过“我所拥有+我所知道”,未来将转向“我的特征+我所知道”。也就是说,之前“我拥有”的u盾、短信验证码+口令等方式,将被替换“我”特有的指纹、声纹、面相+口令等方式。通过新技术的加入最大限度做到只有“我”才能证明“我自己”。

在系统底层建设中,陆光明介绍,目前平台的主流技术仍是基于强密码实现安全保障,并会适时利用安全大数据,进行态势感知的风险预测和控制。对于新兴的区块链技术、时间戳等安全保障方式,平台将做到端口预留。

巨大的用户量是对该平台的另一个严峻考验。据统计,2016年支付宝实名用户达到4.5亿人。与之相比,要构建覆盖中国全体居民以及法人单位的统一身份认证平台,数据处理量可想而知。

为此,亚信安全咨询战略总监吴大明表示,平台在建设和使用的过程中将会不断有新的应用加入,因此平台具备可扩展。一个公民出生、入托再到上学,需要跑到各个地方去办各种手续的体验,未来可能变成可跨省、随时办。

(张佳星)

广告经营许可证:呼工商广字1501004000013 邮编:010010 本报激光照排印刷:呼和浩特日报社印刷厂 本报零售:每份1.6元