亚信陆光明：可信身份体系如何保障网络安全？

身份信息成为互联网安全领域最关键的要素。近日，在成都举办的C3安全峰会上，亚信安全副总裁陆光明认为，面对信息安全的诸多挑战，新的身份认证技术层出不穷，多维度体系、便捷的认证技术、平台级的跨行业之间的传递互认是接下来身份认证的发展趋势。

目前身份体系面临诸多困难，尤其在巨大的商业利益驱动下，窃取网络身份信息并利用已经形成了灰黑产业链，造成非法交易，阻碍正常的网络信息发展。陆光明介绍，不论是在国内外，虚拟网络身份都面临严重的泄露问题。2018年3月持续发酵的Facebook数据泄露事件中有8700万用户资料外泄影响了美国的选举；2011年韩国3500万用户，占95%的韩国网民数据泄露，动摇了韩国网络实名制的基础，导致政府限制网络搜集身份信息；2012年的央视315晚会曝光了罗维邓白氏购买接近一亿的个人信息以进行精准的直复营销。

除了商业机构的信息泄露，网络安全还面临虚假、垃圾注册的问题。2014年11月份开始，国务院办公厅牵头进行全国范围的互联网+政务服务的网上办事大厅，由于缺乏前期良好的顶层规划，各省市或一些区域，政务服务的分散建设形成了大量的非实名注册、垃圾注册。

陆光明指出，目前的认证体系仍有很多缺陷。企业在身份验证的尝试中遇到了身份认证合规性不足、公信力不够、行业受局限、技术缺陷明显等问题。比如中国还在广泛地使用短信验证码，但是该技术非常不安全，无法保证用户身份可信。对于用户而言，每一个系统都必须重复登录，账户负担沉重。为便于记忆，众多账户经常设置相同口令，易遭受撞库攻击。

究竟如何打造可信的身份体系？陆光明表示可信身份认证体系有以下三个趋势发展。第一，单纬度单系统的解决特定场景的可信身份，要向多维度、综合性的可交叉的可信身份体系助力网络安全身份体系发展，并且要形成可信身份认证的传递和互信。

第二，在技术上，安全便捷和身份成本的技术会更加的受青睐，要重视业务的合规性、生物特征的认证、免密无感、融合认证等等。在设备里，内制数字证书或密钥分割协同认证的软认证，是相对更便捷、用户体验更好的认证方法。

第三，可信身份的互联互通需要加强，要调动各方的参与， 需要各行各业的企业、互联网应用的提供商、以及网民的参与，一个以社会公信力的身份认证服务平台则应该作为国家的关键信息基础设施技术来建设。

陆光明表示，建立可信身份体系可借鉴欧盟和美国等国家的经验。2006 年欧盟发布《2010 泛欧洲 eID 管理框架路线图》，开展了网络可信身份体系的立法建设。2011 年美国公布了《美国网络空间可信身份国家战略》，计划用 10 年来建设美国全国的网络身份体系。

在国内，《电子签名法》和《网络安全法》已经搭建了法律和政策的基础建设。网信办，工信部，国家密码管理局等相关部门，也提应当加强顶层设计，推动数据共享，打破数据孤岛，推进电子签名等应用。陆光明呼吁，搭建一个公信力的统一身份认证平台，在身份验证工作中需要先行。只有把它先搭建起来，面向社会的公众和企业，作为统一认证和授权的基础设施，才能提供权威的认证源。

来源：中国反洗钱研究中心网站