第 4 卷◆第 10 期◆版本 1.0◆2022 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

智能门锁风险分析及防范

黄培强
广东顶固集创家居股份有限公司
DOI：10.12238/ems.v4i10.5717

[摘　要] 提出了家用智能门锁的终端及云平台架构，定义了智能门锁中应该保护的用户数据和安全服务内容，对目前面临的信息安全风险进行了剖析，识别出控制单元、生物识别模块、密码键盘等模块面临的信息安全风险，针对智能门锁给出了信息安全风险分析及智能门锁风险防范方法，能够帮助智能门锁厂商在技术选型和方案调研时识别出安全风险。同时，从安全技术方案选取、企业监督、行业共建三个维度提出了提升智能门锁行业的信息安全水平的建议。该研究适用于消费级联网型智能门锁。
[关键词] 智能门锁；风险分析；防范
中图分类号：TP309　文献标识码：A

Risk analysis and prevention of intelligent door lock

Huang Peiqiang
Guangdong Dinggu Jichuang Home Furnishing Co., Ltd

[Abstract] The terminal and cloud platform architecture of household intelligent door lock is proposed, the user data and security services that should be protected in the intelligent door lock are defined, the current information security risks faced are analyzed, the information security risks faced by control units, biometric modules, password keyboards and other modules are identified, and the information security risk analysis and risk prevention methods for intelligent door locks are given, It can help intelligent door lock manufacturers to identify security risks during technology selection and scheme research. At the same time, from the three dimensions of security technology scheme selection, enterprise supervision and industry co construction, the paper puts forward suggestions to improve the information security level of the intelligent door lock industry. This research is applicable to consumer networking smart door locks.
[Key words] intelligent door lock; Risk analysis; to guard against

引言

区别于传统机械锁，智能锁在用户方便性、识别便捷性、管理智能化等方面更具有优势,是门禁系统中锁门的执行部件。相较于欧美国家，我国智能锁产业起步较晚，但发展的速度十分迅猛。特别是随着新一代通信、信息、生物识别等技术的广泛应用，智能锁的功能不断完善，可接入更多的生活场景，智能锁所占的市场份额不断攀升。除了单独销售外，智能锁已成为了防盗安全门、防盗保险柜（箱）等传统安防实体防护产品的标准配置。根据全国锁具行业信息中心发布信息显示，2018年智能锁厂家已超过千家,智能锁生产企业工业总产值超过100亿元。

1、人工智能的发展和涵义

1956年，计算机科学、心理学和经济学的研究人员如马文·明斯基、西摩·派珀特、约翰·麦卡锡、赫伯特·西蒙和艾伦·纽维尔等人在达特茅斯会议上率先提出人工智能的概念。人工智能在20世纪90年代重新流行并迅速发展，目的在于复制并在模式识别和预测方面进行改进(前人工智能时代的计算机在计算和数据处理方面已经优于人类)，包括人脸识别(来自视觉数据)、语音识别(来自听觉数据)、识别日常数据中的抽象模式，以及依据过去的经验和当前的信息做出决策。人工智能领域的突破主要得益于硬件和算法的进步，研究重心表现为人工智能的机器学习方法(使计算机和算法能够从大量数据中学习、预测和执行任务)和深度学习(如神经网络,提高机器学习效率、进行统计推断和优化)。

2、智能锁的安全风险分析

智能锁自进入市场以来，凭借其超强的便捷性已被广大用

户所接受，但很多用户，甚至包括有些制造商对智能锁的安全性要求缺乏足够认识。智能锁搭载的生物识别系统和电子操控系统所带来的安全风险已引起了社会的广泛关注，特斯拉线圈安全风险已引起了社会的广泛关注,导致对特斯拉线圈的恐慌。国家市场监管总局于2018年开展了对智能门锁的质量专项抽查工作，对34批次抽检产品的锁舌伸出长度、锁舌轴向静载荷、锁舌侧向静载荷、执手承受静拉力及扭矩、电源性能、信息保存及误识率、防破坏报警功能、绝缘电阻、泄漏电流、抗电强度和安全性要求等11个项目进行了检验。结果显示，有11个批次不合格，不合格检出率为32.4%，主要涉及锁舌轴向静载荷、电源性能（欠压）、防破坏报警功能、抗电强度等4个项目。导致这些问题的原因是比较复杂的，主要包括智能锁搭载的人脸识别技术尚不成熟，锁具自身的电子防护能力薄弱，在强电场的作用下产生的开锁耦合信号（无线馈电）导致芯片出现逻辑错误等因素。而智能锁的四个机械结构的设计和质量问题所带来的安全性风险同样不容忽视，主要体现在以下方面：1）智能锁面板与执手一般均通过连接头固定，连接头与执手、面板的配合间隙及前、后面板在安全门上的固定方法，都直接影响到产品的使用与安全；2）离合器的设置方式可分为前置、中置与后置，如果防护设计不到位，传动装置极易受到专用工具的攻击；3）主控锁启闭机构在应对轴向静压指标上若没有设置自锁定装置就存在缺陷；4）应急锁启闭机构在防暴力攻击开启性能上存在明显缺陷。此外，智能锁在防盗安全门使用上也存在一些安全隐患。目前，我国现行国家标准《防盗安全门通用技术条件》（GB17565-2007）规定，除主控锁外必须配置付锁和天地栓（甲级门为12个锁定点，乙级门为10个锁定点），这对智能锁的驱动电机的功率和电源都提出了较高的要求。

3、机械结构动态设计概述

机械设计产品整体结构的设计动态分析设计主要流程指的就是通过对各种车床机械设计产品的结构特性特征进行系统分析，对其机械动力学和机械模型结构进行系统建构，并在整个工业机床机械设计技术工作中，能够得到广泛研究运用的一种机械设计工作流程。动态化的仿真机械部件结构模型产品设计，可以对传统产品设计在现阶段中可能发现的一些存在比较薄弱的制造工序和工艺项目，依照产品模型本身所需要仿真的实际状况模型对其进行实时调整和不断改良。在进行内部动态结构设计的工作过程中，不仅应该有效和选择设计变量参数信息，对于初始化的参数和经过修改后的其他参数信息，都应该对此进行不断完善和及时维护，确保各种机械设备产品的内部结构设计动态化和设计运行状况的最佳和优化，对于各种机械设备产品的使用时间表动态设计也应该要对此进行不断强化。为能够确保生产精细化工程机械制造产品的各种动态软件设计技术能够充分满足当下各类机械产品的动态设计应用需要，应该严格地要求确保各种动态产品设计的基本模型和稳定，对其动态设计的操作方法和进行产品设计时的技术流程进行严格规范。

4、构建防范人工智能风险的机制和措施

4.1 以研发人员作为内部风险防范的起点

从防范风险的角度来看，人工智能的挑战在于其研发方式。人工智能系统的设计可在不同的地方和时间进行，而不需要任何有意识的协调，同时内部研发工作可能处于保密状态。危险的人工智能的目的性设计会包括所有其他类型的安全问题，最危险和最难防范的就是故意制造的恶意人工智能。对研发人员实施相应的约束或激励机制，或通过伦理道德培训施加影响，可有效促进研发人员主动追求安全有益的人工智能。

4.2 控制单元保护

为了防范对控制单元的攻击风险，门锁厂商应使用软件数据加密甚至是成本更高的硬加密的方案保护门锁内的敏感数据不被黑客恶意窃取。例如，智能门锁中的密钥、指纹特征值、其他敏感信息等可以保存在安全芯片或者可信执行环境中。此外，远程APP开锁的安全性尚未得到有效保障，所以可在业务允许的情况下禁用远程开锁功能。联网型智能门锁应能将使用过程中产生的输入错误报警、防破坏报警及事件记录等信息上传至后台服务器。在后台服务端，门锁厂商后台服务器不应存储与门锁相匹配的对称密钥信息，防止门锁遭到破解后黑客反向攻击厂商的服务器。

4.3 生物识别模块保护

智能锁内应使用经过权威机构测试认证的安全芯片，加密存储指纹模板和敏感数据。在传输生物识别信息时应该使用足够强壮的加密算法和完善的传输机制。对于假指纹，智能门锁可以考虑使用3D高清图像和指纹算法。

4.4 密码键盘安全保护

智能门锁可采用虚位密码，防止他人偷窥。密码键盘按键表面应该有保护措施,防止黑客在键盘表面安装overlay装置盗取密码。不同的密码键盘按键，其按键声音应该完全一致，防止密码被窃听。如果智能门锁成本允许，应增加主动探测的防拆机制，防止黑客安装物理攻击设备窃取密码。

5、智能锁具设计调研

5.1 智能锁的行业发展空间巨大

锁具发展至今,其历史一直伴随着人类私有财产意识的演变,几乎等同于人类文明的历史。从可以追溯到古代的雏形：绳结、骨档,到如今的各种高科技锁具,锁的出现无疑是文明成熟的主要标志,是文明进步的体现。目前,锁具最重要的变化之一是诞生了新一代产品:智能锁,它是人工智能时代互联网技术和智能识别技术高度融合的产物。智能锁区别于传统锁类的重要特点是在用户体验、家庭防护和管理方面具有更加便捷和安全的性能。不仅是为了生活的智能,也是为了智能锁能够接入物联网,从而进一步构建统一全面的智能家居安全生态网络。因此,在保证高安全性的基础上,灵敏的传感和人性化的服务体验是现代智能锁的前进方向。

5.2 智能锁行业的品牌阵营

随着智能家居市场的迅猛膨胀,许多企业和跨行巨头涌入智能锁行业。根据国家锁具信息中心的数据,2018年中国智能锁

企业数量约为2000家,同比增长67%。品牌结构方面,根据《2019中国智能门锁应用及行业白皮书》,2018年中国智能安防门锁形成品牌聚集效应。目前以德士曼、鹿客等为代表的专业品牌仍是智能锁行业的中流砥柱,以小米、华为智选等为代表的互联网新兴品牌则主要以个体用户公寓门锁为主。

5.3 智能门锁产品的多样化解锁形式

为了增强行业竞争优势,对智能锁技术的研发也在马不停蹄,产品款式也逐渐多元化。目前智能锁以传统手持型为主,2018年传统手持智能锁占比88%,而大部分的推拉式锁安全性能较低,总体的比例不高。传统手持智能锁经常使用密码、指纹、手机等识别方法,但随着人工智能和算法识别相关技术的稳健进步,以及人脸识别、蓝牙解锁、红膜解锁和物联网技术的突破,我国智能安全锁产品的功能和应用将呈现多元化的发展格局。

5.4 智能锁市场竞品分析

通过对目前市面上几家大型家居市场采用走访调查、问卷调查、现场采访的方式,笔者发现目前主流品牌智能锁都采取智能锁和智能猫眼相结合的方式。同时,据获悉资料表明,现有产品目标人群市场大多为包含老年人的三辈人家庭及高薪白领阶层。近年来,单身独居女性对智能锁需求日益增加。进一步整合市场销售情况、品牌、技术现状和未来发展趋势,我们可以得知智能锁需求会日益增加同时其所具备的功能也将更加完善。整体市场发展情况以大品牌为中心,中小品牌为散点环绕式分布,质量参差不齐但发展规模却旗鼓相当;较好地满足了社会各层次人群购买力 。通过用户对各产品的期望值数据,目前备受瞩目的智能锁产品是鹿客智能门锁。2017年鹿客智能门锁的Loock Touch外观和功能上的极简设计一举摘得“智能锁科技创新奖”,实现手握、识别、下压一步即可开门的便利操作,满足用户对美学和人体工学的双重追求;此外还有陨石科技公司研发的夏洛克智能锁贴的防止复制和技术开锁等产品。当前市场主流风向已变为设计驱动创新竞争,为避免陷入为设计而设计的死循环,在市场与设计双重驱动下,注重产品服务过程中的用户体验性是必然趋势 。

结语

智能门锁信息安全研究已成为行业热点，受“小黑盒”攻击事件的影响，消费者也逐渐意识到智能门锁信息安全的重要性，从而驱动了智能门锁厂商加大了对信息安全的投入力度。但是，智能门锁行业发展迅速，安全攻击技术也伴随着行业迅速发展，对应的安全解决方案相对发展速度较慢，其中很重要的原因是缺乏有效的行业引导。未来建议从以下三个层面提升智能门锁行业的信息安全水平。技术层面上，通过构建云端一体化的身份认证方案,向门锁厂商提供安全成本可控的云服务,相比较门锁厂商自建云服务及身份认证管理平台更加迅速和低成平,有助于在短期内提升智能门锁厂商的信息安全水位;从企业层面，尤其是面对消费者的电商平台，需要加大对劣质的、不安全的门锁的管理和监督;行业层面，需要门锁厂商、销售机构、地产厂商、服务提供商及政府加强合作，通过落地项目，引导信息安全方案与智能门锁的融合，帮助提升智能门锁的信息安全程度，提高门锁厂商的信息安全能力，才可以进一步保障智能门锁及其使用者的安全。

[参考文献]

[1] IoT合作伙伴计划联盟. 2017中国智能锁应用与发展白皮书 [Z] . 北京:IoT合作伙伴计划联盟安全组，2017.

[2] ICA/T2018-205-01智能门锁信息安全风险导则[S].北京:IoT合作伙伴计划联盟安全组，2018.

[3]杨京桦. 认清智能门锁十大风险维护产品安全[J]. 中国建设信息化，2018(22):61.

[4]周荆，李青山，陈钟. 智能联网设备身份认证安全风险评估 [J] . 信息安全研究，2018，4(10):881-888.