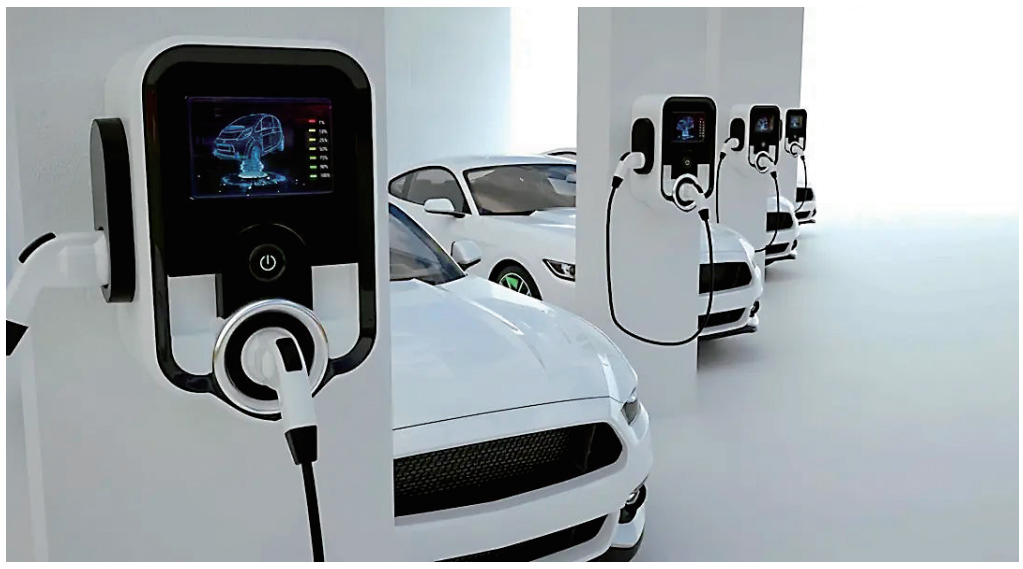
泄露个人信息？

智能充电桩面临信息安全问题

当你对着车机发出“Hi”指令，它可以非常快捷地引导你前往某合作充电桩充电，这个操作过程正成为很多新能源汽车车主的习惯。不过，如此智慧的智能网联，也为充电桩带来了新的安全漏洞。记者留意到，近一年来，不仅国外研究机构对充电桩数据安全发出了警示；在国内，上周，工信部也罕见地通报了部分充电桩平台存在的信息被滥用等问题。

近年，随着新能源汽车渗透率不断提高，充电桩的需求也不断增加，随之而来充电桩的网络安全问题日益凸显，正引发业内高度关注。

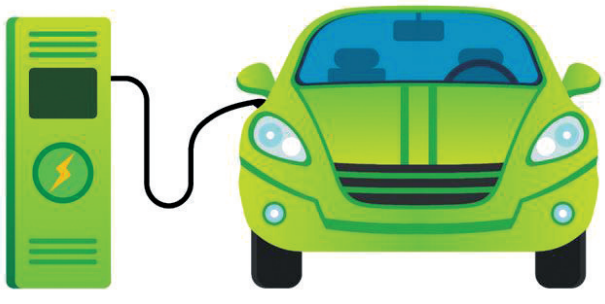

电动汽车充电管理系统受到漏洞的影响。

小心你的“电”会被盗刷

在2022年底上海举办的一场国际安全极客大赛（GeekPwn2020）上，参赛队伍BladeTeam演示了对“无感支付”式直流充电桩的漏洞攻击。利用电动汽车BMS与直流充电桩通信协议中的身份认证漏洞，只需获取受害者的车架号码，即可盗用受害者的账户余额，为其他车免费充电，轻松完成“盗刷”操作。这是近年充电桩信息安全漏洞的一个典型案例示范。今年2月，一家国外知名新能源网络安全公司的研究人员发现多个电动汽车充电管理系统都受到漏洞的影响，可用于“分布式拒绝服务攻击”和窃取驾驶员的敏感信息，包括支付卡数据、服务器凭据等。

充电桩服务商平台对于以上类似的充电安全漏洞有着不可推卸的责任，但事实上，部分平台甚至还存在“监守自盗”的情况。今年5月6日，我国工信部通报了10家企业11款App涉及新能源汽车充换电运营相关的平台存在侵害用户权益的行为，被通报对象包括云能充、小象充、E充站等微信小程序、App。据通报，这些平台所涉问题包括“违规收集个人信息”“强制用户使用定向推送功能”“App强制、频繁、过度索取权限”等。

当前，除了充换电质量和稳定外，用户数据安全已经成为充电桩面临的首要问题。关注大数据安全解决方案的北京创安恒宇调研报告指出：5G、大数据、云计算、区块链、人工智能等数字技术在充电桩领域广泛应用，充电桩产业数字化已成为大势所趋。但与日新月异的智慧技术脱节的是，很多充电桩服务商面对网络的攻击没有招架之力，导致用户数据容易被滥用和泄露。



充电服务商面临网络安全危机

万物互联，为各类应用创新提供了施展的舞台，也因此，充电桩作为电动汽车的首要接口，如今更间接变成了交通信息的收集者、传递者与承载者，而一旦信息泄露，后果严重。业内人士指出，尤其是近年即插即充、无感支付成为充电桩行业的主流发展趋势，风险极大。BladeTeam高级安全研究员Nicky则表示，该团队在国际安全极客大赛上演示的漏洞属于充电通信协议层面缺陷，采用相同技术方案的“无感支付”式直流充电桩均受其影响。此漏洞影响面大、修复难度高，对于行业健康发展具有很强的风险提示价值。

新能源汽车充电安全性和可靠性正成为众多用户以及场站运营商重点关注的部分，目前很多传统充电桩企业对网络安全的防护远远不足。“当前的防护大多集中在新能源车辆电池安全、对充电环境主动监测防护和充换电大数据的对比检测上，如电池散热、失控管理、充电桩‘快充+过充’、电芯质量等问题。”中国软件行业协会智能网联汽车行业分会专家告诉记者，当前智能充电桩系统现有网络边缘尚未建立起完善的本地安全防护能力，无法提供对电桩终端的安全防护。如由于电桩缺少集中管理平台，无法验证恶意访问来源并快速定位被攻击智能充电桩，所以无法即时监控和评估对平台和用户信息资产的威胁状态，并进行分析。

充电桩行业里，很早就关注并着手采用加密技术、数据隔离技术用以确保用户信息安全的Tellus Power集团表示：数据泄露事件暴露出了在很多智能产品大规模投放市场的同时，并未同步建立与之匹配的数据信息安全能力，而这中间的漏洞与缝隙，正变成黑客的乐土。

充电桩不仅要“智能”还需会“防护”

业内人士指出，目前充电站需要统筹管理。北京创安恒宇相关研究人员告诉记者，充电桩或充电站存在点多、面广、分散的特点，其端、管、云均缺少有效的安全防护机制，每个节点都容易遭到入侵，如充电桩自身的系统安全，与本地充电站的数据传输、充电站与运营平台的数据传输，运营平台的平稳运营，用户结算安全等多个领域均存在安全隐患。

中国信息协会信息安全专业委员会副主任李京春指出，严格保护用户隐私数据，平衡数据流通与泄露风险，才能使智能网联汽车产业健康快速发展。当前，充电运营商希望通过收集更多客户信息获取更多客源、更多利润在情理之中，但若被判定为违规收集客户个人信息、触碰了法律，将可能得不偿失。

国家智能网联汽车创新中心信息安全部部长罗承刚指出，数据安全需从监管、标准、管理、技术方面共同推进。

对于充电桩信息安全防御能力问题，有业内专家指出，保障用户数据的安全，需采取多项措施。首先，在设计产品之初，就要充分考虑数据安全风险，并采用加密技术来保护用户的隐私，如对充电桩的信息读取过程、数据传输过程的加密。其次，建议定期进行数据备份和恢复演练，确保数据不会丢失或被破坏。最后，与第三方安全公司合作，对充电桩进行定期安全检查，确保系统的稳定性和可靠性。

频发的信息网络泄露风险，也开始让企业意识到需升级充换电领域的安全防护领域。如吉利旗下的极氪能源ZEEKR Power电动汽车交流充电桩，近期宣布成为首个通过中国网络安全审查技术与认证中心安全评估，获得“IT产品信息安全认证证书”的充电桩产品。据企业介绍，除了常见的短路、漏电、过压、联机等保护多重防护设计外，最重要的是，该充电桩具备完善的信息安全技术保障，能够及时发现、报告并处理网络攻击或异常行为。

华为近年来也在发力充电桩产品，相关负责人告诉记者，华为构建了“云管边端”的架构体系和产品解决方案，从芯片、操作系统、数据库、到端到端可信安全技术，且都是自主可控，有效实现能源智能化，和数据信息安全防护。此外，东风、广汽等相关车企针对智能汽车的网联系统等采用双安全组件，支持功能安全最高的ASIL D级，智能网联云平台采用国密级别数据安全保护算法，个人敏感数据脱敏处理，保证用户数据安全。

（据《广州日报》）