德安全专家破解手机GSM加密算法思科认证 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/644/2021_2022__E5_BE_B7_E5_AE_89_E5_85_A8_E4_c101_644388.htm GSM最初开发于1988年，迄今已有21年的使用历史，目前全球80%约35亿部在用手机使用GSM技术，是应用最广泛的手机标准。GSM 系统采用的是名为A5/1的64位加密技术。在诺尔眼中，这种加密简直太弱了，通过他提供的破解表（需要高配置计算机算十年获得），专用软件，一根天线和 30000美元左右的硬件，就可以实时破解密码，监听通话。而记录通话内容，也花不了多少钱。况且这种设备不仅已有现成的供应商，专供政府机关，而且通过开源硬件也可以组装。而在诺尔的最新技术公布之前，破解A5/1只是理论上可能，因为需要的硬件设备非常昂贵。两类攻击设备诺尔表示，自己之所以要破解GSM加密算法纯属学术行为，目的是找出该技术目前存在的漏洞，并最终促使业界提高GSM技术的安全标准。因为在美国即使讨论窃听工具也是违法的，研究人员一般不会去从事类似的研究。但诺尔在咨询了电子前线基金会的律师之后，找到了一种自信没有违法的办法：设立一个开源项目，只提供破解表生成程序，而不设计破解设备。（该开源项目的具体技术细节可以访问这个网站。）诺尔表示，虽然这本身不合法，但是有经验的黑客确实有可能利用它进行违法犯罪活动。事实上，两年前已经有两名黑客从事过类似的研究，但没有最后完成。他本人使用的是黑莓GSM手机，现在他不会通过手机来交流机密信息了。GSM协会的反应代表各大GSM手机厂商和运营商利益的GSM联盟（GSM Association）早在今年8

月就得知了这一消息。但是他们当时表示，诺尔的小组动机不纯，背后可能有其他商业利益，而且他们可能低估了破解的复杂性，离实际得手尚早。这实际上将诺尔等研究人员置于尴尬的境地，一方面，他们因为法律限制无法公开讨论，而另一方面，黑客们所需的工具完全是可以公开获取的。后来在这几天媒体曝光的压力之下，GSM联盟又转而表示：会严肃处理此事，将组织专家进行研究，并强调上述破解活动属于非法行为。但协会对诺尔声称的为了促进用户通信安全而进行的破解活动，表示无法理解。专家反应加州伯克利大学的教授David Wagner表示，他对此并不惊奇。事实上，早在1997年，学术界就已经找到了理论上的破解。但诺尔的研究证明破解比原来预想的还要容易。现在的确该从 GSM转到更安全的系统了。人们不会总是这么幸运，在威胁发生之前就得到警告。当然，有条件的单位比如政府，可能早已经在监听手机通讯。安全权威Bruce Schneier否定了GSM联盟不负责任的声明。他说，目前攻击的威胁不是减弱，而是越来越强了。同时他也表示，虽然手机可能被监听影响很大，但现在更严重的问题是用GSM来支付和身份验证。新一代算法也不安全用于3G上的加密算法也是由GSM协会开发的，名为A5/3，据称更加安全。但是，诺尔在讲座中演示，这个算法学术上也已经被破解，并得到了仿真验证。两种加密算法使用了同样的密钥，从而削弱了安全性。对A5/3的破解手法是所谓半主动攻击（semi-active attack），所需工具都可以公开获得。【诺尔简介】今年28岁的诺尔2008年毕业于美国弗吉尼亚大学，获得了计算机工程博士学位。博士论文题为Implementable Privacy for RFID Systems。目前住在柏林，主

要研究兴趣是小设备的安全性。今年早些时候，他还查找出无绳电话加密算法存在的安全漏洞，并促使标准组织DECT论坛对原有安全标准加以升级。