

物流考试综合辅导：德国RFID安全专家揭露电子护照新漏洞  
PDF转换可能丢失图片或格式，建议阅读原文

[https://www.100test.com/kao\\_ti2020/250/2021\\_2022\\_\\_E7\\_89\\_A9\\_E6\\_B5\\_81\\_E8\\_80\\_83\\_E8\\_c31\\_250059.htm](https://www.100test.com/kao_ti2020/250/2021_2022__E7_89_A9_E6_B5_81_E8_80_83_E8_c31_250059.htm) 去年，德国一位安全研究者展示如何克隆电子护照中的芯片，现在该专家又揭露了电子护照和读取它们的检测系统存在着其他的安全漏洞。RFID专家Lukas Grunwald是德国国会电子护照的安全顾问。Lukas近日称生物电子护照存在的安全漏洞使非法获取、克隆指纹成为可能，犯罪人员可以利用偷盗来的指纹创建特定编码的芯片，用于攻击读取它的阅读器。Grunwald称通过克隆护照芯片，他已经成功攻击了不同厂家制造两种护照阅读器，修改了包含护照相片的JPEG2000 图片文件。读取修改后的图片破坏了阅读器，这意味着阅读器易受code-injection exploit黑客技术的攻击，如对读取器重新编辑，使过期护照或假护照也能通过。Grunwald计划于本周末在拉斯维加斯举行的年度DefCo黑客大会上讨论这个问题。电子护照中包含一个RFID芯片，政府希望以此防止伪造通关文件上，并加快通关速度。美国是推行电子护照的先锋国家。但是Grunwald在去年的黑帽安全大会上就展示了如何从只读取的护照芯片中获取数据，并将数据克隆到可读写芯片上，护照阅读器读取结果是一样的。现在Grunwald称他可以在克隆芯片中增加数据，以对护照阅读器进行攻击。Grunwald没有透露受攻击的阅读器厂商，但是他称目前这两款阅读器已应用在一些机场的出入检测点。100Test 下载频道开通，各类考试题目直接下载。详细请访问 [www.100test.com](http://www.100test.com)