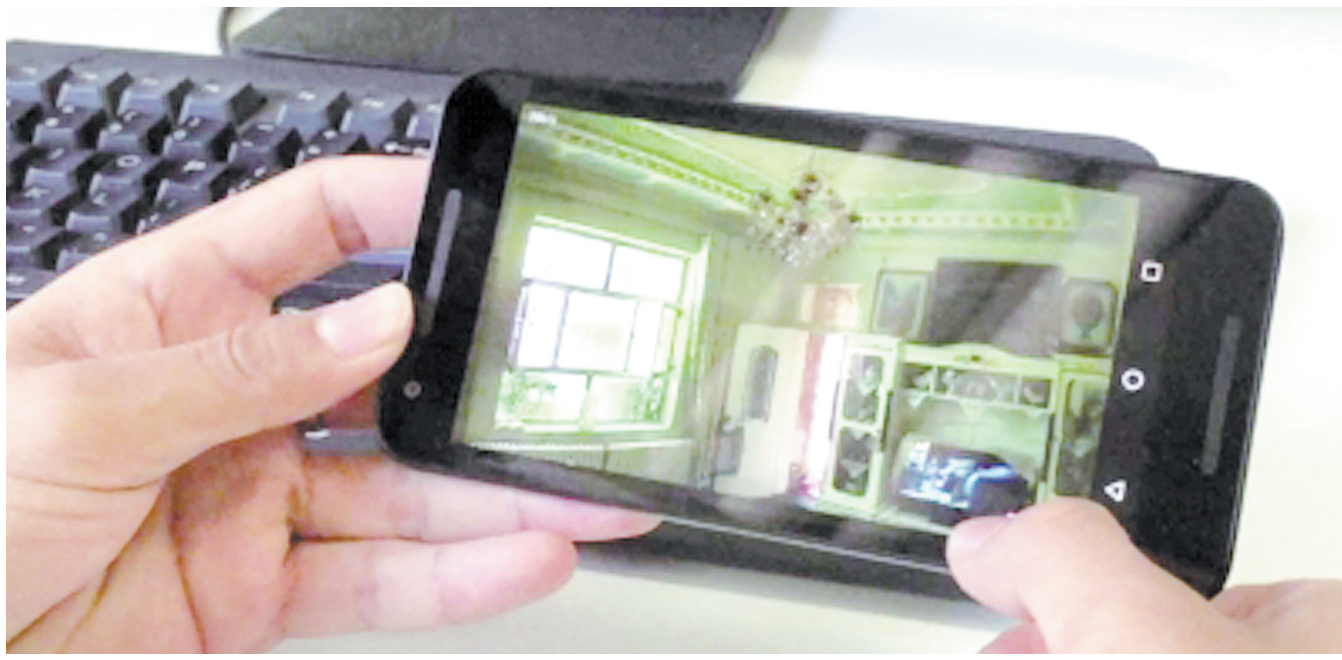


通过手机能看到别人家的摄像内容。

工程师演示获取家用智能摄像头用户实时画面全过程

八成家用智能摄像头存泄密风险

近日，有多名网友反映，自己在家中安装了家用智能摄像头后，出现个人信息、室内场景画面被泄露等现象，疑与摄像头及其附属软件有关。5月10日下午，一位专业工程师向记者现场演示了获取家用智能摄像头用户信息及实时画面的全过程，并证实个别品牌摄像头确实存在泄密可能。据了解，根据相关测试结果，目前市场上近八成家用智能摄像头产品存在安全缺陷。

■案例

客厅照片外泄被挂网上

张女士家住海淀，她和老公白天都要上班，家中两岁半儿子无人照料，所以聘请了一名全职保姆照看。为能够实时掌握儿子在家的信息，夫妻俩于今年3月末通过网站购买了一组某知名品牌的远程监控摄像头，并安装在客厅、卧室、厨房等多个位置。

然而，就在今年4月中旬，张女士在浏览某小型家居网站时，无意间发现自家客厅的截图被挂在网页上。张女士称，在此之前，她和家人从来没邀请或允许任何网站的人到家中拍照片，“照片的角度就是从挂摄像头的位置拍摄的，而且画质、颜色都和手机APP上的实时画面一模一样。”此后，张女士设法与该网站取得了联系，对方很快将网上照片删除。“对方说，图片不是他们拍摄的，而是从网上下载的，我继续追问图片来源，对方拒绝回答。”

张女士称，图片中没有出现儿子和保姆的影像，“应该说并没有出现特别严重的隐私泄露情况，可是这个隐患实在太可怕了，如果是卧室的画面泄露，那后果不堪设想。”

“我们怀疑和家里装的摄像头有关。”无奈之下，张女士只能将所有摄像头和相应的手机APP全部卸载。

■实验

破解代码窃取实时画面

针对频频出现的家用智能摄像头泄密现象，某实验室在对国内市场上销售的近百个品牌的家用摄像头进行了安全评估测试后发现，市面上不少品牌的摄像头，存在用户信息泄露、数据传输未加密等安全缺陷，甚至可以在用户毫不知情的情况下，直接实时观看用户摄像头拍摄的内容并录像。

5月10日下午，实验室安全研究员王先生，为记者演示了通过软件漏洞获取已绑定手机用户摄像头实时画面的全过程。记者发现，王先生所使用的工具仅为一台已经联网的电脑，一部手机以及一段自行编写的代码。

演示过程开始前，王先生首先在手机上下载了某品牌家用摄像头的APP软件，随后注册账号，但并没绑定任何摄像头，此时其页面中摄像头列表显示为空。

随后，王先生在电脑软件上输入刚刚注册的账号、密码，并在电脑上运行其编写的代码。随着代码的运行，手机APP页面上立即出现多个摄像头监控画面的预览图，且随着时间的推移数量逐渐增多，随机点开其中一个，经过短暂加载，摄像头远程传输的画面开始播放，且清晰度相当高，甚至可以辨别用户家电视中播放的电视画面。除此，在代码脚本运行过程中，大量用户注册时使用的手机号码也一同显示在屏幕上。

王先生表示，通过视频中的不同场景可以明显看出，这些画面并不仅限于某一个用户安装的摄像头的拍摄画面。“如果需要的话，(别有用心的人)可以将所有注册此APP的用户信息全部弄出来，然后根据单个用户的手机号码定位到某个特定用户身上”，从而实施针对性极强的个别用户信息窃取活动。而只要轻轻点击手机APP软件上的录制按钮，盗取的画面就会轻松地保存下来。

而对于这段作为工具的代码，王先生称，只要有一定编程知识和经验的人都可以完成，并不存在特别高的技术门槛，“就现在而言，能够编写这种代码的人还是很多的。”

■结论

八成家用摄像头存在安全漏洞

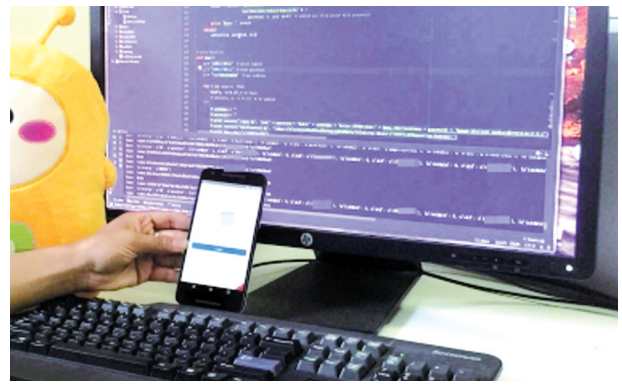
在一份题为《摄像头横向测试表》的文件中记者发现，技术人员对目前市面上多个品牌的摄像头，进行了“手机控制终端”、“云端应用安全”、“设备终端安全”三个大项30多个小项的测试，结果所涉猎品牌均或多或少存在安全问题。

安全研究员王先生告诉记者，从测试结果来看，目前，有关视频画面泄露的问题主要集中在摄像头软件云端逻辑漏洞和手机APP软件漏洞两个方面，“其他可能导致信息泄露的问题也存在，但是相比之下数量较少。”

王先生所在的实验室在对国内市场上销售的近百个品牌的家用智能摄像头进行安全评估测试后发现，近八成产品存在用户信息泄露、数据传输未加密、APP未安全加固、代码逻辑存在缺陷、硬件存在调试接口、可横向控制等安全缺陷。

据安全工程师刘健皓介绍，这些安全缺陷的存在让接入网络的摄像头可以轻易被不法分子控制，随时获取摄像头的图像和语音信息，对安装摄像头的家庭或公司进行监控甚至网上直播。

刘健皓解释，从理论上讲，通过手机远程查看到摄像头内容，必须通过注册，甚至要求“一对一”。但是，个别品牌的摄像头与手机进行连接时，并没有对手机身份进行验证，这是一个非常严重的漏洞。黑客可以通过漏洞，用一个虚拟的绑定就可以查看数百个摄像头实时画面，而出现此漏洞的摄像头至少有数十款，其中包括了一些著名品牌。



电脑输入代码后通过手机观看。

■建议

有关部门须建立摄像头安全标准

针对如何能够保障用户使用家用智能摄像头拍摄的个人隐私不被泄露的问题，软件安全工程师提醒广大用户，首先在购买摄像头时，应对所选品牌进行一些调查，可以通过互联网查询与目标品牌相关的帖子或报道，“目的就是找到一个口碑不错，价格也合适的品牌”。

第二，在使用时，要注意设置一定强度的密码，及时关注摄像头软件的提醒。如果绑定的手机上发现了请求验证码的短信，就应该立刻修改密码。

第三，经常登录摄像头进行查看，如发现实际拍摄角度与安装时发生变化等情况，就需要考虑自己的账号安全了。同时，要关注所用品牌摄像头安全方面的消息，如果发现设备漏洞应停止使用，等待厂家更新，并保证所使用的摄像头软件是最新版本。

与此同时，安全工程师还针对家用智能摄像头行业提出了建议。首先，有关部门亟须建立一套针对智能摄像头的信息安全标准。其次，建议智能硬件开发商建立自己的运营平台，以保护消费者的数据安全，及时发现并阻断黑客的攻击。最后，需要制定一套有效的应急响应预案，确保在安全漏洞出现后，能够快速响应，并最大程度降低用户的损失。

■说法

技术偷窥侵犯个人隐私算犯法

针对频频出现的家用智能摄像头泄露个人隐私事件，北京雄志律师事务所律师姜健表示，个人住宅属于自然人较为私密的生活空间，有权利根据个人意愿公开或不公开，即所谓的隐私权。如果有人利用信息技术手段远程控制他人安装在室内摄像头，非经权利人同意而获取他人住宅内生活信息，虽然手段新颖，但本质上仍属于偷窥行为，侵犯了他人的隐私权。

根据我国治安管理处罚法的相关规定，偷窥、偷拍、窃听、散布他人隐私的，处5日以下拘留或者500元以下罚款；情节较重的，处5日以上10日以下拘留，可以并处500元以下罚款。如通过偷窥形式获得的他人私密照片，并上传到网络平台，或者出售获利的，将涉嫌构成刑事犯罪。另外，被侵权人有权向侵权人主张民事赔偿责任。

（据京华时报）