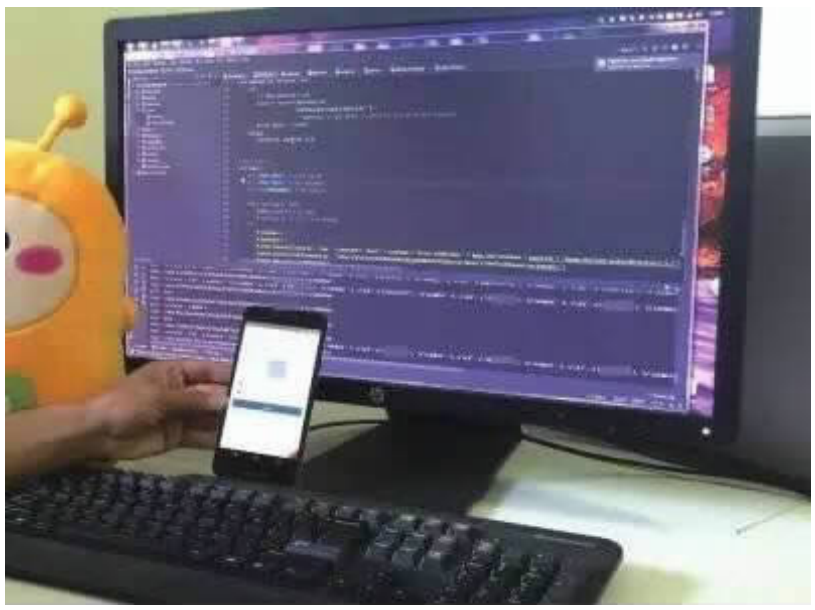

电脑输入代码后通过手机观看。

通过手机能看到别人家的摄像内容。

八成家用智能摄像头泄密风险大 可随时遭远程窃取图像、语音信息

日常生活中，不少人在家中安装摄像头。然而近日多名网友反映，自己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。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

今年3月末，北京市海淀区的张女士网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。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

破解代码可窃取实时画面

安全研究员王先生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，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。

他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。

结论

八成家用摄像头存在安全漏洞

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。

关注三湘都市报微信看E报。

建议

使用家用智能摄像头注意这三点

第一，购买时应对所选品牌进行一些调查，通过互联网查询与目标品牌相关的帖子或报道，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。

■来源于央视新闻 微信号 cctvnewscenter