



UNCLASSIFIED//FOR OFFICIAL USE ONLY

624TH OPERATIONS CENTER
INTELLIGENCE SURVEILLANCE & RECONNAISSANCE DIVISION



Cyber Threat Bulletin

23 September 2013 (Issue 143)

Prepared/edited by 624 OC/ISRD (AFCYBER)

The Cyber Threat Bulletin is designed to keep Air Force members knowledgeable of user & network threats. It is located on the AF Portal. It's against our policy to send out this bulletin or request personal data via email. Sources are provided for reference outside official channels.

Hackers Expose “Smart Home” Vulnerabilities

As technology's ever growing capabilities continue to expand at a rapid and impressive rate, so do the ways in which we use that technology. Home automation, or “Smart House,” technology enables remote management of home security and surveillance systems, IP enabled door locks, IP enabled lights, smart home appliances, HVAC, and more. Unfortunately, however, it also presents a vulnerability for hackers to exploit.



At the recent Black Hat conference, computer researchers demonstrated multiple vulnerabilities “Smart Homes” present to hackers. These included how they could remotely unlock a deadbolt, disarm a home-security system, open a garage door, turn lights on and off, and turn a smart TV into a camera.

These cyber security professionals were able to achieve the above effects because all of these gadgets are internet capable;

something many consumers are increasingly taking for granted. This is especially applicable to the users that are now incorporating smartphones, tablets, and laptops into their lives to control certain facets of their everyday surroundings.

It is important to remember that in the excitement of new technology, we cannot forget about the security concerns that come with them. For your safety, it is advised to do

UNCLASSIFIED//FOR OFFICIAL USE ONLY

research on possible security vulnerabilities of any home automation technology you may be thinking of adding to your household.

(Source: online.wsj.com, Symantec.com)



Apple iPhone iOS 7 Lockscreen Bypass Vulnerability

The latest version of the iPhone's operating system currently offers a gaping hole in its old-fashioned passcode lock screen. Videos have surfaced online showing how to take advantage of this vulnerability.

Anyone can exploit the bug by swiping up on the lockscreen to access the phone's "control center," and then open the alarm clock. Holding the phone's sleep button brings up the option to power it off with a swipe. Instead, the intruder can tap "cancel" and double click the home button to enter the phone's multitasking screen. That offers access to the phone's camera and stored photos, along with the ability to share those photos from the user's accounts, essentially allowing anyone who grabs the phone to hijack the user's email, Twitter, Facebook, or Flickr account.

The best option to mitigate the lockscreen vulnerability is to wait to update your iPhone until Apple has published a patch fixing this gaping security vulnerability. If you have already updated your iPhone, don't be alarmed. There is a quick mitigation technique for you as well.

iPhone users can prevent the control center from appearing on their lockscreen by accessing "settings," then "control center." Once in the "control center" application click the "Off" position. iPhone users should be aware of this major security vulnerability and then make an educated decision about updating the iOS. (Source: forbes.com)

For any security related questions, issues, or concerns, contact your Unit Information Assurance Officer, Wing IA and/or the Information Protection Office.

Do you have a question, comment, or concern? Have a topic you would like to see in a future bulletin? Feel free to call us at DSN: 969-0137, or e-mail us at 624oc.isrd@lackland.af.mil. The use or omission of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the Air Force.

To receive automatic notification of each new Cyber Threat Bulletin loaded to the AF Portal, select the "Set an Alert" button at the top of the Cyber Threat Bulletins Archive page.