Gmail by Google

Karen West <karenwest15@gmail.com>

Update in Thread - Here is an interesting case which boarders on being a hardware security issue - Hardware Security

Hardware Security Course Staff <noreply@coursera.org> Thu, Feb 19, 2015 at 3:02 PM
To: Karen West <KarenWest15@gmail.com>

Karen West,
Dan Cogan has written a new post in the thread Here is an interesting case which boarders on being a hardware security issue on the General Discussion forum for the Hardware Security online course.

Someone mentioned to me the other day about the idea that a compiler could inject extra code into your binary than you intended. When was the last time you checked your binary to make sure extra code isn't in there!? I'm not saying that's the case here, although seems like a nice way to get around the problem of engineers updating their firmware. Instead, make sure when engineers update their compiler, that they get a version which as the code injector built in. Also wouldn't be noticed by CRC checks.

And as you proposed, a synthesis tool (or other back-end tools) for hardware could inject trojan logic as well.

You mentioned TV - There's an article that discusses Samsung's use of microphones in their smartTVs. They warn that conversations near the

microphone used for voice recognition may be picked up. No one knows if these conversations are kept or not, but we can imagine. Not sure how long this link will be around, but for what its worth :http://www.cnbc.com/id/102407345

Click here to view the post. Subscribe to it to get notified when a response comes in.

Thanks,
The Hardware Security Course Staff

Go to Forum