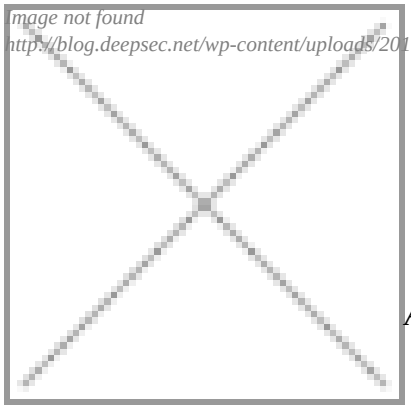
DeepSec Talk 2017: Normal Permissions In Android: An Audiovisual Deception – Constantinos Patsakis

Posted on **October 17,2017** by **sanna**

The Marshmallow version was a significant revision for Android. Among the new features that were introduced one of the most significant is, without any doubt, the runtime permission. The permission model was totally redesigned, categorising the permissions into four main categories. The main concept of this categorisation is how much risk a user is exposed to when permissions are granted. Therefore, normal permissions imply the least risk for the user. However, in this case, there are some important issues. Firstly, these permissions are not actually displayed to the user; they are not displayed upon installation and the user needs to dig into several menus to find them for each app. Most importantly though, these permissions cannot be revoked. Unlike permissions categorized as dangerous, where the user can grant or revoke a permission whenever deemed necessary, the normal permissions are automatically granted and cannot be revoked, unless the user uninstalls the app that uses them. The research question that arises from this change is whether the apps that request only normal permissions are benign. Note that an app requesting only normal permissions will never request any alerting action from the user, hence the user is more probable to install it and not to worry about it. Furthermore, since these permissions are automatically granted, this means that any malicious action that could be made with such permissions can be ported to any installed app as they will not require any user interaction.

In his talk at DeepSec 2017 Constantinos Patsakis will show several attacks that can be launched by such applications ranging from overlays and tapjacking to recording audio without requesting any permission categorised as dangerous.

Update: Google has issued an update for some of the issues presented in this talk. The patch is only for „premium“ users as described in thissecurity bulletin for the Pixel/Nexus models.



Assistant Professor Constantinos Patsakis holds a B.Sc. in Mathematics from the University of Athens, Greece and a M.Sc. in Information Security from Royal Holloway, University of London. He obtained his PhD in Cryptography and Malware from the Department of Informatics of University of Piraeus. His main areas of research include cryptography, security, privacy, data anonymization and data mining.

He has authored more than 70 publications in peer reviewed international conferences and journals and he has been teaching computer science courses in European universities for more than a decade. Dr Patsakis has been working in the industry as a freelance developer and security consultant. He has participated in several national (Greek, Spanish, Catalan and Irish) and European R&D projects. Additionally, he has worked as researcher at the UNESCO Chair in Data Privacy at the Rovira i Virgili University (URV) of Tarragona, Catalonia, Spain and as a research fellow at Trinity College, Dublin Ireland. Currently, he is Assistant

Professor at University of Piraeus and adjunct researcher of Athena Research and Innovation Center.

Posted in:Conference,Security | Tagged:Android,DeepSec,Marshmallow,Mobile,Talk | With 0 comments