Privacy Breakthrough Emerges for Smartphone Messaging

Dean Blakely Software launches first messenger in the world to run without dangerous permissions

Tucson, Arizona, May 14, 2017 -- Until now, anyone that wanted to use an end-to-end encrypted messenger had to forfeit over total control of everything on their phone. This issue has become one of the biggest privacy concerns in the messaging sphere. But now, a new messenger has just been released that requires no permissions to access any data at all and still accomplishes end-to-end encrypted messaging. This is a first.

As privacy becomes a subject of more concern, Google has attempted to address the issue by reorganizing permissions on Android devices into “normal” and “dangerous” categories. The dangerous permissions are indeed dangerous as they can give an app total control over everything on an Android phone. The owner of the phone has no idea what’s going on.

The issue is scary. Permissions demanded by today’s most popular messaging apps enable draconian authority. The apps can read everything on the phone and give or sell that data to anyone. It is not unusual for these messengers to demand 20 to 30 dangerous permissions.

They could email all of the videos on a phone to all of the contacts. Start the microphone and download what is being said at the time, know what is looked at on any page on the internet, copy pictures taken and mail them to anyone, know everywhere the phone goes and when, who is called and when, how long the call lasted, etc.

The new messenger is SafeTalk Encrypted Messenger from Dean Blakely Software. Gary Blakely, the principal at the company when asked why he developed it said “I don’t like or trust any of the messengers on the market. So, I took it upon myself to write a totally safe, honest, stealth messenger that everyone could trust. We have proven that stealth encrypted messaging can be done without violating the phone it runs on.”

When asked if he thinks the other vendors such as Signal and WhatsApp might be selling the data they have access to, Gary said “I’m not going to accuse anybody of trafficking in stolen data. We are proving that we don’t do it by not being able to do it. SafeTalk has made this whole issue a non-issue. Users don’t have to worry about it anymore.”

When asked about income projections we were told “It’s up in the air. A big majority of app users don’t care at all about privacy. The Facebook generation wants their lives out there for everyone to see. SafeTalk will appeal to the more serious business type of user. This is not a social media toy. This is a messenger you could bet your life on.”

The Dean Blakely marketing material (http://www.deanblakely.com/safetalk.pdf) points out other features of the SafeTalk messenger in addition to the lack of permission demands. It’s advertised to be the only messenger where the user can remain totally anonymous if desired – no phone numbers or Google Account numbers are solicited.

SafeTalk also allows a user to disassemble their un-obfuscated executable and examine the very code that runs on their phone. They publish an “auditing guide” to make this process easier for any user with questions. The goal here is for someone to prove to themselves that their plain-text message is not being mistreated in any way.

Another very interesting feature is language translation – Gary said “the two people communicating don’t have to speak the same language. Currently eight languages are available. These eight languages machine translate very well if the text is kept simple.”

Website Link: http://droid.deanblakely.com
Google Play Link: https://play.google.com/store/apps/details?id=com.deanblakely.SafeTalk
Send an email to: Gary@deanblakely.com
520-906-1592
###