How do I know what SafeTalk is really doing with my message?

We do not obfuscate our code that runs on the phone because we want you to be able to "decompile" the code and look at it and see exactly what it is doing. You will be looking at the exact code from the very .APK module that runs on your phone. We also produce PDF documents showing the code with explainations of what it is doing.

What you care about is that the message you enter gets encrypted the instant you hit the send button and that the un-encrypted message never leaves the phone. Our docs highlight that exact string of code proving beyond a doubt that your message is safe.

We realize that people's lives might depend on the safety of their messages.

There are a few things you should be aware of . . .

- If you use the Adroid microphone to speak your message, your message is sent to the Google Servers to convert your voice to text. Therefore those servers see your clear un-encrypted message. You might want to consider typing your very critical messages.

- If your cooreespondant is receiving your message in another language, the Google or Bing servers are used to translate say English to French and, of course this takes place on the receiving phone after the message has been decrypted. So the translator feature may reduce message safety.

- By default SafeTalk saves all messages in plain text on both the sending and receiving phones. They are organized into conversation threads just like your SMS messaging app. If a message is critical you might want to delete it soon after you send it. Same logic for the receipient. If you are worried about the receiptient's judgement you can send a "Vanishing Message" that will only last one minute on the receiving phone. (SafeTalk disables screen copy).

We think SafeTalk is, by far, the easiest messaging app to audit and this includes the so called Open Source systems. All of the "heavy lifting" code in SafeTalk is done on our servers. The Android code is actually small and easy to understand.