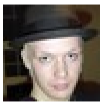
BUZZ CHRONICLES > TECH
Saved by @Mollyycolllinss
See On Twitter

Twitter Thread by Ola Bini



Ola Bini
@olabini

I posted about the Signal messaging application versus Telegram a while ago, and I received a lot of answers about different applications as alternatives. So I'd like to write a thread giving an overview about my perspective on the security of different applications. 1/53

It's very important to remember that this thread is only about messaging applications for mobile phones, and the evaluations are based on my own perspectives and needs. In some cases they will be subjective, and you should investigate before applying the advice to yourself. 2/53

As I've mentioned in previous, when talking about secure messaging applications, it's extremely important to remember that if an application is secure enough, the limitation will not be the security of the application itself, the limitation is the security of the device. 3/53

When talking about security, the weakest link in a chain will be the one an attacker will go after. There are some applications in this thread that are very secure and have great protocols. But if the device is compromised, that will simply not matter. 4/53

So, if you have something very sensitive to discuss, my strong advice is to not trust that information to a mobile device - there are simply too many ways it could be compromised. So, from that perspective, the security of the protocol is not relevant. 5/53

Of course, a messaging application can _fail_ by not having good enough security, but once you reach a certain level, the security of the protocol or the application is not a factor anymore. As always, figure out a threat model for your situation before deciding. 6/53

This list will not be in any particular order. I will try to keep the summaries fairly concise to make this thread smaller than a hundred tweets. In general, you might have to dig deeper for further information, or ask for clarifications. So, let's jump in! 7/53

First, Confide. Confide has been around since 2013. It was early supporting disappearing messages. Confide is not open source, which disqualifies it for me. Security audits have also found many issues over the years, so although it's end-to-end encrypted, it's not for me. 8/53

OK, Facebook Messenger. I basically consider the mobile applications for FB messenger spyware. They've had a long history of asking for much more permissions than necessary, and using questionable methods for collecting all kinds of user information. 9/53

The application is obviously also closed source, making it impossible to inspect. These days, the applications does support end-to-end encryption, but this is optional. It does use the Signal protocol for this feature, which is good. That said, I wouldn't recommend it. 10/53

What about the different Google messaging products? Things like Allo, Duo, Hangouts and all the others? You might see the trend by now - these are all closed source. Some of them support end-to-end encryption at some level, but usually as an optional mode. 11/53

When it comes to Google products, the opaqueness of their implementation, combined with lack of clarity of product evolution and uncertain security properties, I would recommend simply staying away from them. 12/53

OK, so what about Apple's iMessage? Any better? Just as the others we've just looked at, it's a proprietary and closed source tool. What's more, it's only available on Apple products. On the other hand, Apple has been quite open about how certain parts of it works. 13/53

Independent analysis of the security properties of iMessage has been done. What are the results? My summary would be "meh". The end-to-end encryption seems to work well enough, but there are certainly ways around it if Apple took an interest in a certain customer. 14/53

This might be a good place to pause and talk about backups. If you do any kind of cloud backups for a mobile messaging application, it's often the case that your messages will _not_ be protected the same way (or at all) they are in the application. 15/53

For this reason, this evaluation doesn't really look at what happens if you have backups turned on. It's the same kind of situation as if an adversary has their hands on your unlocked phone - in general you lose. 16/53

The same thing is completely true if an adversary has managed to infect your phone with malware - especially if that malware has succeeded in countering the security mitigations on your phone and achieved kernel access. In this situation, you lose. 17/53

It's important to remember this. We talked about the security of mobile phones in the beginning of the thread, but I want to remind you. There are many types of attacks that an application simply can't protect you against. Don't put too sensitive information on your device. 18/53

What about Session? This is a very new messenger application at the moment. It is open source and doesn't require real-world identifiers (such as phone number) to register. It tries very hard to be decentralized, and removing as much meta data as possible in the design. 19/53

To be honest, Session looks quite interesting. It's pushing forward in directions that other messenger solutions are not. However, it is also very new, has not been audited yet, and it's unclear how well it scales in practice. It's also built on new protocols. 20/53

For all of these reasons, I would not recommend using Session for anything critical at the moment. It's a project worth keeping an eye on, and in a while it might be something I would recommend - but security also has to be conservative, Session is too new. 21/53

Time to look at Signal. First, the good parts. It has a very good end-to-end encrypted protocol. Encryption also covers groups, although not with the same security properties as one-on-one. In general, there's a lot of functionality, and adoption is high. 22/53

Signal is completely open source, both the clients and the server. Their security choices are generally conservative in a positive way, while still evaluating new technology to solve problems such as backups and privacy contact discovery. 23/53

Buuuuuuuut. Signal still requires phone numbers for registration, and will automatically notify you when someone in your contact list signs up. There are still bugs here and there - and the app still crashes often, at least for some users. 24/53

Just a few days ago, Signal was completely down for roughly 12 hours, because of a huge surge in new users. This could happen to anyone, of course, but it still must have given a bad impression to all those new people, fleeing WhatsApp. 25/53

What about security? In general, it's pretty good, for running on a phone. There are persistent discussions about information leaks through Google's Android keyboard, or through third party installed keyboards. But honestly, I think Signal is doing the right thing here. 26/53

If a user installs a custom keyboard, they expect to be able to use it everywhere. Taking away that choice would be actively hostile to a good user experience. And when it comes to GBoard, it seems to me that if Google is your adversary, you shouldn't use a Google OS. 27/53

Same thing is true for iOS and Apple, of course. If your threat model is such that you can't trust the basic services of the phone, you should not put anything sensitive on that phone. It's not just keyboards - these providers have a million ways to backdoor you. 28/53

So from my perspective, being worried about the keyboard doesn't really make sense. It comes from an inconsistent threat model. 29/53

Since we are talking about messaging applications, let's just look at regular text messages - SMS. Not encrypted, transmitted over the air and with no real delivery control of any kind, it's really the worst of all options. 30/53

Now Telegram... As I mentioned in an earlier tweet, Telegram should _not_ be considered a secure messaging application. Yes, it supports end-to-end encryption, but it's not turned on by default, and the design is such that cryptographers go "hmmmm". And not in the good way. 31/53

Telegram groups are also very popular - but they are not encrypted at all. Further, the Telegram is open source - which is good - but the servers are not. Overall, I would recommend that you stay away from Telegram, especially if you have any security needs. 32/53

OK, what about Threema? There are things to like about this application. They have good documentation about their security, focus on privacy is strong, their group design is such that it hides most information even from the servers. No phone number needed for registration. 33/53

However, there are also some issues. First, and most importantly, it's not open source. And while they have received several audits, that's not nearly the same thing. Their marketing material is also quite misleading at times, most importantly regarding forward secrecy. 34/53

Specifically, they claim that Threema is forward secret, but looking at the protocol documentation it turns out that it's only the _transport layer_ which has forward secrecy, not the actual end-to-end encryption. 35/53

I guess now is a good time to discuss the issue of jurisdiction. Many people talk about the benefits of messenger applications being based in Switzerland, because of the strong privacy laws found there. My personal opinion is that jurisdiction doesn't actually help. 36/53

There are simply too many ways around jurisdiction from a legal protection standpoint. I prefer technology and cryptography to protect me. If jurisdiction is something you think you can depend on, any one of the messenger applications in this thread should work for you. 37/53

And then we come to the elephant in the room - WhatsApp. First, WhatsApp is not really a choice in many parts of the world. Most people in Latin America relies on WhatsApp to such a large degree that you almost have to have it installed, if you live here. 38/53

Now, WhatsApp has a huge market penetration. They do have end-to-end encryption, based on the Signal protocol. Usability is pretty good as well, and there are many features, including things like business accounts and so on. 39/53

However, WhatsApp is not open source, and it's owned by Facebook. It's clear that they collect a large amount of meta data and traffic information -and that this is very valuable to them. The recent fracas about changed terms and conditions doesn't actually change anything. 40/53

Instead, these new terms and conditions only clarify things that WhatsApp was _already_ doing. While having WhatsApp installed is sadly something you might not get away from, I recommend using other alternatives as much as possible, and certainly for sensitive things. 41/53

OK, on to Wickr. This was a very early adopter of "disappearing messages". You can see how cool it is if you've ever seen Mr Robot. However, while disappearing messages are useful, they are not the strong security measure you might imagine. 42/53

Wickr has decent cryptography, as far as we can tell - but this goes to the core of the problem again: we can't verify this, since Wickr is not open source. This reason is enough for me to feel uncomfortable recommending Wickr. 43/53

Our final entry in this list is Wire. Of all the messenger applications, I think Wire is the one that most people claim as the one you should use instead of Signal. A lot of this support comes from the fact that Wire doesn't require phone numbers for registration. 44/53

Another common argument for Wire is the legal residence, since Wire was created in Switzerland. But you have already seen my thoughts on that above. And that's also less relevant now, since in 2019 the company that owns Wire was bought by a US corporation... 45/53

What about crypto? Wire is based on the Signal protocol, using libsodium for their implementation. Nothing complicated or problematic here. Wire has also open sourced both their client and server software, which makes it easier to verify the system. 46/53

However, there are other security considerations that continue to be concerning. Audits have uncovered problems and some of those have been fixed, while others remain - such as sending of passwords over a simple TLS connection. 47/53

But the most problematic aspect of Wire in my opinion has to do with their policies around data retention. Their servers store much more information than necessary, and lots of meta-data about users are stored completely unencrypted. 48/53

Finally, Wire does not support group messaging at all (in the Wire Personal version). Taking all of these things together, especially data retention and change of ownership, makes me feel quite uncomfortable using Wire for anything sensitive. 49/53

We have reached the end. The truth is, none of these options are fantastic. All have issues and I can't recommend any single one without caveats. I personally do use Signal as my main messenger application, since on balance, it suits my threat model best. 50/53

But I need to reiterate - you don't put anything sensitive on a mobile device in the first place. If you do, it doesn't really matter which secure messenger you use, since all of them runs on a device which have security limitations. 51/53

One final point, which might be obvious - all of these evalutions are based on some assumptions. One of them is that you actually install the real application. In some cases there have been reports about people downloading a messenger and being attacked by it. 52/53

These things can always be traced back to a situation where the download happened from a place that wasn't official. Of course, in sensitive enough situations, backdoored applications can concievably be served by app stores as well. Once again: don't trust mobile devices. 53/53