Katzenpost Zine episode 0x00: what is anonymous communication? Q & A

dawuud

Fall 2023

We are all under more surveillance than ALL of human history!

We conclude that the age old communications privacy problem hasn't yet been solved. There is no modern and effective strongly anonymous communications network. The old methods of protecting our privacy might not have the strongest security guarantees compared to using modern end to end encryption like Signal, WhatsApp. But at least the old methods don't snitch about who you are communcating with; whereas Signal and WhatsApp by design cannot prevent the identities of your communication correspondants from being discovered by adversaries who compromise the communications infrastructure.

The katzenpost team is a group of cypherpunks that are dedicated to building strongly anonymous communications networks that everyone can use to communicate more freely.

To quote the cypherpunk's manifesto:

"Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free for all to use, worldwide. We don't much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down. "

There is not any solution right now that we'd recommend except to say that if you really are a person in a very high risk situation with very powerful adversaries, then you had better not use ANY modern communications infrastructure in your communications with your communication correspondents.

Old school technology still works but doesn't have strong confidentiality guarantees. Use the night's cover of darkness, whispers, envelopes, closed doors, secret handshakes, couriers and dead drops.

What is anonymous communication?

Anonymous communication allows us to communicate more freely because it protects the identities or geographical locations of the people we are communicating with, from the operators of the communications infrastructure.

Currently, Tor is the most successful anonymous communication network. However, it has very weak anonymity properties which can be trivially broken by sufficiently global passive adversaries.

A sufficiently global passive adversary is any adversary or set of colluding adversaries (e.g. the set of cooperating nation states + drug cartels + corporations) who are able to observe your entry and exit, into and out of the Tor network.

Simple statistical correlation is made between your input and output packets flowing into and out of the Tor network.

Tor is not strong anonymity.

The people operating our communications infrastructure get to learn who our friends are, their geographical locations and our frequency of communications etc.

In practice, this information is available to the large powerful nation states because they can simply gag order and subpoena the communications infrastructure operators.

End to end encryption of your communications is important, however services and communication programs like Signal, Wire and WhatsApp do indeed give us end to end encryption.

That's not good enough. All the above metadata is still leaked, the man learns with whom you are communicating with because that cannot be "encrypted".

We're all under more surveillance than all of human history because of our recent adoptions of modern technology. Pretty much all current communications technology leaks metadata such as:

- geographical location
- message sender
- message receiver
- message send time
- message receive time
- size of the message
- message sequence