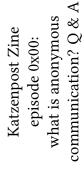


Fall 2023

dawuud

what is anonymous Katzenpost Zine episode 0x00:





lance than ALL of human history!

There is no modern and effective strongly anony-

tions privacy problem hasn't yet been solved. mous communications network. The old methstrongest security guarantees compared to us-WhatsApp. But at least the old methods don't snitch about who you are communicating with; whereas Signal and WhatsApp by design can-

We conclude that the age old communica-

ods of protecting our privacy might not have the

"Cypherpunks write code. We know that some

punks that are dedicated to building strongly anonymous communications networks that ev-

eryone can use to communicate more freely.

To quote the cypherpunk's manifesto:

The katzenpost team is a group of cypher-

one has to write software to defend privacy, and since we can't get privacy unless we all do, we're our fellow Cypherpunks may practice and play

going to write it. We publish our code so that with it. Our code is free for all to use, world-

ing modern end to end encryption like Signal

not prevent the identities of your communication correspondants from being discovered by

wide. 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 dis-

persed system can't be shut down."

adversaries who compromise the communica-

ions infrastructure.

We are all under more surveil-

What is anonymous communication?

are communicating with, from the operators of tities or geographical locations of the people we municate more freely because it protects the iden

adversary or set of colluding adversaries (e.g. tels + corporations) who are able to observe your the set of cooperating nation states + drug car-A sufficiently global passive adversary is any

sApp 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 can-

munication programs like Signal, Wire and What tions is important, however services and com-

End to end encryption of your communica-

tructure operators.

der and subpoena the communications infrasthe FBI, NSA because they can simply gag ortheir geographical locations and our frequency

The people operating our communications

In practice, this information is available to

the communications infrastructure.

communications technology leaks metadata such of modern technology. Pretty much all current human history because of our recent adoptions

We're all under more surveillance than all of

geographical location

trivially broken by sufficiently global passive advery weak anonymity properties which can be mous communication network. However, it has Currently, Tor is the most successful anony-

entry and exit, into and out of the Tor network.

size of the message

 message receive time message send time message receiver message sender

message sequence

your input and output packets flowing into and Simple statistical correlation is made between

in your communications with your collaboraa person in a very high risk situation with very use ANY modern communications infrastructure powerful adversaries, then you had better not There is not any solution right now that we'd

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