Glossary

Choosing a private messenger requires the understanding of many technical terms, that many users, even quite technical, often misunderstand. This list is aiming to fill this knowledge gap. Please suggest any changes or additions.

While this glossary aims to be factual and objective, it is not completely unbiased. We designed SimpleX to be the most private, secure and resilient communication network, and some definitions reflect this view.

Address portability

Similarly to phone number portability (the ability of the customer to transfer the service to another provider without changing the number), the address portability means the ability of a communication service customer to change the service provider without changing the service address. Many federated networks support SRV records to provide address portability, but allowing service users to set up their own domains for the addresses is not as commonly supported by the available server and client software as for email.

Anonymous credentials

The credential that allows proving something, e.g. the right to access some resource, without identifying the user. This credential can either be generated by a trusted party or by the user themselves and provided together with the request to create the resource. The first approach creates some centralized dependency in most cases. The second approach does not require any trust - this is used in SimpleX network to authorize access to the messaging queues.

Digital credential on Wikipedia

Blockchain

In a wide sense, blockchain means a sequence of blocks of data, where each block contains a cryptographic hash of the previous block, thus providing integrity to the whole chain. Blockchains are used in many communication and information storage systems to provide integrity and immutability of the data. For example, BluRay disks use blockchain. SimpleX messaging queues also use blockchain - each message includes the hash of the previous message, to ensure the integrity – if any message is modified it will be detected by the recipient when the next message is received. Blockchains are a subset of Merkle directed acyclic graphs.

In a more narrow sense, particularly in media, blockchain is used to refer specifically to distributed ledger, where each record also includes the hash of the previous record, but the blocks have to be agreed by the participating peers using some consensus protocol.

Wikipedia

Break-in recovery

Post-compromise security.

Centralized network

Centralized networks are provided or controlled by a single entity. The examples are Threema, Signal, WhatsApp and Telegram. The advantage of that design is that the provider can innovate faster, and has a centralized approach to security. But the disadvantage is that the provider can change or discontinue the service, and leak, sell or disclose in some other way all users' data, including who they are connected with.

Content padding

Message padding.

Decentralized network

Decentralized network is often used to mean "the network based on decentralized blockchain". In its original meaning, decentralized network means that there is no central authority or any other point of centralization in the network, other than network protocols specification. The advantage of decentralized networks is that they are resilient to censorship and to the provider going out of business. The disadvantage is that they are often slower to innovate, and the security may be worse than with the centralized network.

The examples of decentralized networks are email, web, DNS, XMPP, Matrix, BitTorrent, etc. All these examples have a shared global application-level address space. Cryptocurrency blockchains not only have a shared address space, but also a shared state, so they are more centralized than email. Tor network also has a shared global address space, but also a central authority. SimpleX network does not have a shared application-level address space (it relies on the shared transport-level addresses - SMP relay hostnames or IP addresses), and it does not have any central authority or any shared state.

Defense in depth

Originally, it is a military strategy that seeks to delay rather than prevent the advance of an attacker, buying time and causing additional casualties by yielding space.

In information security, defense in depth represents the use of multiple computer security techniques to help mitigate the risk of one component of the defense being compromised or circumvented. An example could be anti-virus software installed on individual workstations when there is already virus protection on the firewalls and servers within the same environment.

SimpleX network applies defense in depth approach to security by having multiple layers for the communication security and privacy:

- double ratchet algorithm for end-to-end encryption with perfect forward secrecy and post-compromise security,
- additional layer of end-to-end encryption for each messaging queue and another encryption layer of encryption from the server to the recipient inside TLS to prevent correlation by ciphertext,
- TLS with only strong ciphers allowed,
- mitigation of man-in-the-middle attack on client-server connection via server offline certificate verification,
- mitigation of replay attacks via signing over transport channel binding,
- multiple layers of message padding to reduce efficiency of traffic analysis,
- mitigation of man-in-the-middle attack on client-client out-of-band channel when sending the invitation,
- rotation of delivery queues to reduce efficiency of traffic analysis,
- etc.

Wikipedia

Double ratchet algorithm

It is used by two parties to exchange end-to-end encrypted messages. The parties will use some key agreement protocol to agree on the initial shared secret key.

Double Ratchet algorithm provides perfect forward secrecy and post-compromise security. It is designed by Signal, and used in SimpleX Chat and many other secure messengers. Most experts consider it the state-of-the-art encryption protocol in message encryption.

End-to-end encryption

A communication system where only the communicating parties can read the messages. It is designed to protect message content from any potential eavesdroppers – telecom and Internet providers, malicious actors, and also the provider of the communication service.

End-to-end encryption requires agreeing cryptographic keys between the sender and the recipient in a way that no eavesdroppers can access the agreed keys. See key agreement protocol. This key exchange can be compromised via man-in-the-middle attack, particularly if key exchange happens via the same communication provider and no out-of-band channel is used to verify key exchange.

Wikipedia

Federated network

Federated network is provided by several entities that agree upon the standards and operate the network collectively. This allows the users to choose their provider, that will hold their account, their messaging history and contacts, and communicate with other providers' servers on behalf of the user. The examples are email, XMPP, Matrix and Mastodon.

The advantage of that design is that there is no single organization that all users depend on, and the standards are more difficult to change, unless it benefits all users. There are several disadvantages: 1) the innovation is slower, 2) each user account still depends on a single organization, and in most cases can't move to another provider without changing their network address – there is no address portability, 3) the security and privacy are inevitably worse than with the centralized networks.

Federation on Wikipedia

Forward secrecy

Also known as perfect forward secrecy, it is a feature of a key agreement protocol that ensures that session keys will not be compromised even if long-term secrets used in the session key exchange are compromised. Forward secrecy protects past sessions against future compromises of session or long-term keys.

Wikipedia

Key agreement protocol

Also known as key exchange, it is a process of agreeing cryptographic keys between the sender and the recipient(s) of the message. It is required for end-to-end encryption to work.

Wikipedia

Key exchange

Key agreement protocol.

Man-in-the-middle attack

The attack when the attacker secretly relays and possibly alters the communications between two parties who believe that they are directly communicating with each other.

This attack can be used to compromise end-to-end encryption by intercepting public keys during key exchange, substituting them with the attacker's keys, and then intercepting and re-encrypting all messages, without altering their content. With this attack, while the attacker does not change message content, but she can read the messages, while the communicating parties believe the messages are end-to-end encrypted.

Such attack is possible with any system that uses the same channel for key exchange as used to send messages - it includes almost all communication systems except SimpleX, where the initial public key is always passed out-of-band. Even with SimpleX, the attacker may intercept and substitute the key sent via another channel, gaining access to communication. This risk is substantially lower, as attacker does not know in advance which channel will be used to pass the key.

To mitigate such attack the communicating parties must verify the integrity of key exchange - SimpleX and many other messaging apps, e.g. Signal and WhatsApp, have the feature that allows it.

Wikipedia.

Merkle directed acyclic graph

Also known as Merkle DAG, a data structure based on a general graph structure where node contains the cryptographic hashes of the previous nodes that point to it. Merkle trees are a subset of Merkle DAGs - in this case each leaf contains a cryptographic hash of the parent.

This structure by design allows to verify the integrity of the whole structure by computing its hashes and comparing with the hashes included in the nodes, in the same way as with blockchain.

The motivation to use DAG in distributed environments instead of a simpler linear blockchain is to allow concurrent additions, when there is no requirement for a single order of added items. Merkle DAG is used, for example, in IPFS and will be used in decentralized SimpleX groups.

Wikipedia.

Message padding

Also known as content padding, it is the process of adding data to the beginning or the end of a message prior to encryption. Padding conceals the actual message size from any eavesdroppers. SimpleX has several encryption layers, and prior to each encryption the content is padded to a fixed size.

Wikipedia.

Onion routing

A technique for anonymous communication over a computer network that uses multiple layers of message encryption, analogous to the layers of an onion. The encrypted data is transmitted through a series of network nodes called "onion routers," each of which "peels" away a single layer, revealing the data's next destination. The sender remains anonymous because each intermediary knows only the location of the immediately preceding and following nodes.

The most widely used onion network is Tor.

Some elements of SimpleX network use similar ideas in their design - different addresses for the same resource used by different parties, and additional encryption layers. Currently though, SimpleX messaging protocol does not protect sender network address, as the relay server is chosen by the recipient. The delivery relays chosen by sender that are planned for the future would make SimpleX design closer to onion routing.

Wikipedia

Overlay network

Nodes in the overlay network can be thought of as being connected by virtual or logical links, each of which corresponds to a path, perhaps through many physical links, in the underlying network. Tor, for example, is an overlay network on top of IP network, which in its turn is also an overlay network over some underlying physical network.

SimpleX Clients also form a network using SMP relays and IP or some other overlay network (e.g., Tor), to communicate with each other. SMP relays, on another hand, do not form a network.

Wikipedia

Pairwise pseudonymous identifier

Generalizing the definition from NIST Digital Identity Guidelines, it is an opaque unguessable identifier generated by a service used to access a resource by only one party.

In the context of SimpleX network, these are the identifiers generated by SMP relays to access anonymous messaging queues, with a separate identifier (and access credential) for each accessing party: recipient, sender and and optional notifications subscriber. The same approach is used by XFTP relays to access file chunks, with separate identifiers (and access credentials) for sender and each recipient.

Peer-to-peer

Peer-to-peer (P2P) is the network architecture when participants have equal rights and communicate directly via a general purpose transport or overlay network. Unlike client-server architecture, all peers in a P2P network both provide and consume the resources. In the context of messaging, P2P architecture usually means that the messages are sent between peers, without user accounts or messages being stored on any servers. Examples are Tox, Briar, Cwtch and many others.

The advantage is that the participants do not depend on any servers. There are multiple downsides to that architecture, such as no asynchronous message delivery, the need for network-wide peer addresses, possibility of network-wide attacks, that are usually mitigated only by using a centralized authority. These disadvantages are avoided with proxied P2P architecture.

Wikipedia.

Perfect forward secrecy

Forward secrecy.

Post-compromise security

Also known as break-in recovery, it is the quality of the end-to-end encryption scheme allowing to recover security against a passive attacker who observes encrypted messages after compromising one (or both) of the parties. Also known as recovery from compromise or break-in recovery. Double-ratchet algorithm has this quality.

Post-quantum cryptography

Any of the proposed cryptographic systems or algorithms that are thought to be secure against an attack by a quantum computer. It appears that as of 2023 there is no system or algorithm that is proven to be secure against such attacks, or even to be secure against attacks by massively parallel conventional computers, so a general recommendation is to use post-quantum cryptographic systems in combination with the traditional cryptographic systems.

Wikipedia

Privacy

Someone's right to keep (or the state when they keep) their personal matters and relationships secret (e.g., Cambridge dictionary). Privacy of communication systems should include the privacy of connections and meta-data, not only the privacy of the content of messages. End-to-end encryption on its own does not provide privacy, as it only protects message content and not connections or meta-data.

Wikipedia

Proxied peer-to-peer

Network topology of the communication system when peers communicate via proxies that do not form the network themselves. Such design is used in Pond, that has a fixed home server for each user, and in SimpleX, that uses multiple relays providing temporary connections.

Recovery from compromise

Post-compromise security.

User identity

In a communication system it refers to anything that uniquely identifies the users to the network. Depending on the communication network, it can be a phone number, email address, username, public key or a random opaque identifier. Most messaging networks rely on some form of user identity. SimpleX appears to be the only messaging network that does not rely on any kind of user identity - see this comparison.