SoK: Secure Messaging

Nik Unger Sergej Dechand Joseph Bonneau Sascha Fahl
Henning Perl Ian Goldberg Matthew Smith

March 20, 2024

Presented by: Georgios Gotzias , Dimitrios Kogios
National Technical University of Athens

Summary

1. Motivation
2. Goal of the paper
3. Threat model
4. Desirable Properties
5. Trust Establishment
6. Conversation Security
7. Transport Privacy
8. Conclusions

Motivation

Motivated by revelations of widespread state surveillance of personal communication, many solutions now claim to offer secure and private messaging.

Motivation

Motivated by revelations of widespread state surveillance of personal communication, many solutions now claim to offer secure and private messaging.

However the intense pressure in the past years to deliver solutions quickly has resulted in subpar results:

- Incomplete objectives

Motivation

Motivated by revelations of widespread state surveillance of personal communication, many solutions now claim to offer secure and private messaging.

However the intense pressure in the past years to deliver solutions quickly has resulted in subpar results:

- ◇ Incomplete objectives
- ◇ Dubious security claims

Motivation

Motivated by revelations of widespread state surveillance of personal communication, many solutions now claim to offer secure and private messaging.

However the intense pressure in the past years to deliver solutions quickly has resulted in subpar results:

- ◇ Incomplete objectives
- ◇ Dubious security claims
- ◇ A lack of broad perspective on the existing literature

Goal of the paper

The Evaluation and Systematization of current solutions as well as the proposal of an evaluation framework based on of the following key points:

Goal of the paper

The Evaluation and Systematization of current solutions as well as the proposal of an evaluation framework based on of the following key points:

- **Trust establishment** : Key distribution and proof of association with the owing entity.

Goal of the paper

The Evaluation and Systematization of current solutions as well as the proposal of an evaluation framework based on of the following key points:

- **Trust establishment** : Key distribution and proof of association with the owing entity.
- **Conversation security** : Protection of exchanged messages.

Goal of the paper

The Evaluation and Systematization of current solutions as well as the proposal of an evaluation framework based on of the following key points:

- **Trust establishment** : Key distribution and proof of association with the owing entity.
- **Conversation security** : Protection of exchanged messages.
- **Transport privacy** : Protection of communication metadata.

Threat model

In order to evaluate the security and privacy that different approaches provide we must consider a variety of adversaries both passive and active:

Threat model

In order to evaluate the security and privacy that different approaches provide we must consider a variety of adversaries both passive and active:

- **Local Adversary** : an attacker controlling local networks.

Threat model

In order to evaluate the security and privacy that different approaches provide we must consider a variety of adversaries both passive and active:

- **Local Adversary** : an attacker controlling local networks.
- **Global Adversary** : an attacker controlling large segments of the Internet, such as powerful nation states or large internet service providers.

Threat model

In order to evaluate the security and privacy that different approaches provide we must consider a variety of adversaries both passive and active:

- **Local Adversary** : an attacker controlling local networks.
- **Global Adversary** : an attacker controlling large segments of the Internet, such as powerful nation states or large internet service providers.
- **Service providers** : For messaging systems that require centralized infrastructure (e.g., public-key directories), the service operators should be considered as potential adversaries.

Threat model

In order to evaluate the security and privacy that different approaches provide we must consider a variety of adversaries both passive and active:

- **Local Adversary** : an attacker controlling local networks.
- **Global Adversary** : an attacker controlling large segments of the Internet, such as powerful nation states or large internet service providers.
- **Service providers** : For messaging systems that require centralized infrastructure (e.g., public-key directories), the service operators should be considered as potential adversaries.

We assume that all adversaries are participants in the messaging system, allowing them to start conversations, send messages, or perform other normal participant actions.

Desirable Properties

The approaches that will be evaluated will be given points if they hold specific properties:

Desirable Properties

The approaches that will be evaluated will be given points if they hold specific properties:

- **Security and Privacy**

Desirable Properties

The approaches that will be evaluated will be given points if they hold specific properties:

- **Security and Privacy**
- **Usability** : Human end users need to understand how to use the system securely and the effort required to do so must be acceptable for the perceived benefits.

Desirable Properties

The approaches that will be evaluated will be given points if they hold specific properties:

- **Security and Privacy**
- **Usability** : Human end users need to understand how to use the system securely and the effort required to do so must be acceptable for the perceived benefits.
- **Ease of Adoption** : Protocols might introduce adoption issues by requiring additional resources or infrastructure from end users or service operators.

Trust Establishment

Definition

The process of users verifying that they are actually communicating with the parties they intend.

Trust Establishment

Definition

The process of users verifying that they are actually communicating with the parties they intend.

This includes both *long-term key exchange* i.e users sending keys to each other and *long-term key authentication* i.e allowing users to ensure that cryptographic keys are associated with the correct real-world entities.

Trust Establishment

Desirable Security and Privacy properties

- *Network MitM Prevention* : Prevents Man-in-the-Middle (MitM) attacks by local and global network adversaries.
- *Operator MitM Prevention* : Prevents MitM attacks executed by infrastructure operators.
- *Operator MitM Detection* : Allows the detection of MitM attacks performed by operators after they have occurred.
- *Operator Accountability* : It is possible to verify that operators behaved correctly during trust establishment.
- *Key Revocation Possible* : Users can revoke and renew keys.
- *Privacy Preserving* : The approach leaks no conversation metadata to other participants or even service operators.

Trust Establishment

Desirable Usability properties

- *Automatic Key Initialization*: No additional user effort is required to create a long-term key pair.
- *Low Key Maintenance* : Some systems require that users sign other keys or renew expired keys. Usable systems require no key maintenance tasks.
- *Easy Key Discovery* : When new contacts are added, no additional effort is needed to retrieve key material.
- *Easy Key Recovery* : Easy to revoke old keys and initialize new keys.
- *Inattentive User Resistant* : Users do not need to carefully inspect information (e.g., key fingerprints) to achieve security.
- Many more... No Shared Secrets , Alert-less Key Renewal , Immediate Enrollment...

Trust Establishment

Desirable Adoption properties

- *Multiple Key Support* : Users should not have to invest additional effort if they or their conversation partners use multiple public keys
- *No Service Provider Required* : Trust establishment does not require additional infrastructure (e.g., key servers).
- *Asynchronous* : Trust establishment can occur asynchronously without all conversation participants online.
- *Scalable* : Trust establishment is efficient, with resource requirements growing logarithmically (or smaller) with the the total number of participants in the system.

Opportunistic Encryption (baseline)

- An encrypted session is established without any key verification.

Trust Establishment

Evaluation

Opportunistic Encryption (baseline)

- An encrypted session is established without any key verification.
- Countering passive adversaries.
- Can't protect from MitM attacks.
- Provides all usability and adoptability features.

Trust Establishment

Evaluation

Opportunistic Encryption (baseline)

- An encrypted session is established without any key verification.
- Countering passive adversaries.
- Can't protect from MitM attacks.
- Provides all usability and adoptability features.

TOFU (Trust-On-First-Use)

- Extends baseline approach by remembering previously seen keys.

Trust Establishment

Evaluation

Opportunistic Encryption (baseline)

- An encrypted session is established without any key verification.
- Countering passive adversaries.
- Can't protect from MitM attacks.
- Provides all usability and adoptability features.

TOFU (Trust-On-First-Use)

- Extends baseline approach by remembering previously seen keys.
- Providing partially the network MitM prevented and infrastructrure MitM prevented properties.
- *Strict form:* Providing inattentive user resilience.
- *Non-strict form:* Providing easy key recovery.

Trust Establishment

Evaluation

Authority-based Trust

Public keys must be vouched by a trusted authority

Trust Establishment

Evaluation

Authority-based Trust

Public keys must be vouched by a trusted authority

Public-key directories

- Providing key revocation.
- Can't protect from MitM attacks by the authority.
- Providing nearly all usability and adoptability features.

Trust Establishment

Evaluation

Authority-based Trust

Public keys must be vouched by a trusted authority

Public-key directories

- Providing key revocation.
- Can't protect from MitM attacks by the authority.
- Providing nearly all usability and adoptability features.

Certificate authority schemes

- Key revocation is impractical.
- But provides the privacy preserving feature.

Trust Establishment

Evaluation

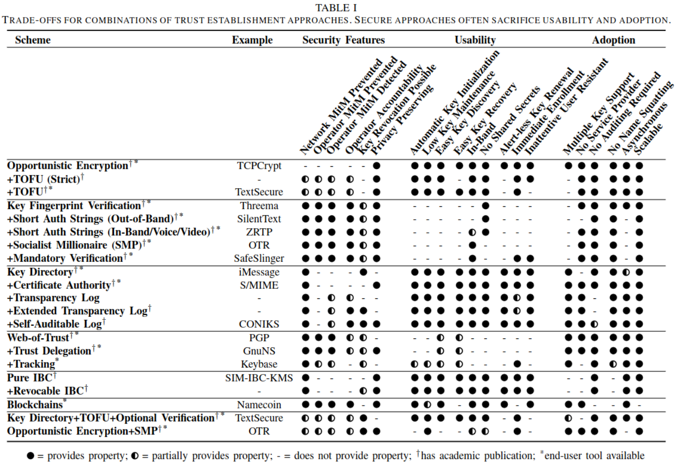

TABLE I

TRADE-OFFS FOR COMBINATIONS OF TRUST ESTABLISHMENT APPROACHES. SECURE APPROACHES OFTEN SACRIFICE USABILITY AND ADOPTION.

Scheme	Example	Security Features						Usability									Adoption					
		Network MitM Prevented	Operator MitM Prevented	Operator MitM Detected	Operator Accountability	Key Revocation Possible	Privacy Preserving	Automatic Key Initialization	Low Key Maintenance	Easy Key Discovery	Easy Key Recovery	In-Band	No Shared Secrets	Alert-less Key Renewal	Immediate Enrollment	Inattentive User Resistant	Multiple Key Support	No Service Provider	No Auditing Required	No Name Squatting	Asynchronous	Scalable
Opportunistic Encryption†*	TCPCrypt	-	-	-	-	-	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
+TOFU (Strict)†	-	◐	◐	◐	◐	-	●	●	●	●	-	●	●	-	●	●	-	●	●	●	●	●
+TOFU†*	TextSecure	◐	◐	◐	◐	-	●	●	●	●	●	●	●	-	●	-	-	●	●	●	●	●
Key Fingerprint Verification†*	Threema	●	●	●	●	◐	●	-	-	-	-	-	●	-	-	-	-	●	●	●	●	●
+Short Auth Strings (Out-of-Band)†*	SilentText	●	●	●	●	◐	●	-	-	-	-	-	●	-	-	-	-	-	●	●	-	●
+Short Auth Strings (In-Band/Voice/Video)†*	ZRTP	●	●	●	●	◐	●	-	-	-	-	◐	●	-	-	-	-	●	●	●	-	●
+Socialist Millionaire (SMP)†*	OTR	●	●	●	●	◐	●	-	-	-	-	●	-	-	-	-	-	●	●	●	-	●
+Mandatory Verification†*	SafeSlinger	●	●	●	●	◐	●	-	-	-	-	●	-	-	●	●	-	●	●	●	-	●
Key Directory†*	iMessage	●	-	-	-	●	-	●	●	●	●	●	●	●	●	●	●	-	●	●	◐	●
+Certificate Authority†*	S/MIME	●	-	-	-	-	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●
+Transparency Log	-	●	-	◐	◐	-	-	●	●	●	●	●	●	●	◐	●	●	●	-	●	●	●
+Extended Transparency Log†	-	●	-	◐	●	●	-	●	●	●	●	●	●	●	◐	●	●	●	-	●	●	●
+Self-Auditable Log†	CONIKS	●	-	◐	●	●	●	●	●	●	●	●	●	●	●	●	●	●	◐	●	●	●
Web-of-Trust†*	PGP	●	●	●	◐	◐	-	-	-	◐	◐	-	-	-	-	-	●	●	●	●	●	●
+Trust Delegation†*	GnuNS	●	●	●	◐	◐	●	-	-	◐	◐	-	-	-	-	-	●	●	●	●	●	●
+Tracking*	Keybase	●	◐	◐	-	◐	-	◐	◐	◐	◐	-	-	-	●	-	●	-	●	◐	●	●
Pure IBC†	SIM-IBC-KMS	●	-	-	-	-	●	●	●	●	●	●	●	●	●	●	-	-	●	-	●	●
+Revocable IBC†	-	●	-	-	-	◐	●	●	●	●	●	●	●	●	●	●	-	-	●	-	●	●
Blockchains*	Namecoin	●	●	●	●	-	●	●	◐	●	-	●	●	●	-	●	●	●	-	-	●	-
Key Directory+TOFU+Optional Verification†*	TextSecure	◐	◐	◐	◐	●	-	●	●	●	●	●	●	-	●	-	◐	-	●	●	●	●
Opportunistic Encryption+SMP†*	OTR	◐	◐	◐	◐	●	●	-	●	-	-	◐	◐	-	●	-	●	●	●	●	-	●

● = provides property; ◐ = partially provides property; - = does not provide property; †has academic publication; *end-user tool available

Figure: Evaluation of different trust establishment approaches

Trust Establishment

Discussion

- No trust establishment approach is perfect.

Trust Establishment

Discussion

- No trust establishment approach is perfect.
- Approaches either sacrifice security and provide a nearly ideal user experience, or sacrifice user experience to achieve nearly ideal security scores.

Trust Establishment

Discussion

- No trust establishment approach is perfect.
- Approaches either sacrifice security and provide a nearly ideal user experience, or sacrifice user experience to achieve nearly ideal security scores.
- It may be wise to start from the basic user experience of today's widely deployed communication apps and try to add as much security as possible, rather than start from a desired security level and attempt to make it as simple to use as possible.

Trust Establishment

Discussion

- No trust establishment approach is perfect.
- Approaches either sacrifice security and provide a nearly ideal user experience, or sacrifice user experience to achieve nearly ideal security scores.
- It may be wise to start from the basic user experience of today's widely deployed communication apps and try to add as much security as possible, rather than start from a desired security level and attempt to make it as simple to use as possible.
- The approaches with good security properties should focus on improving usability.

Conversation Security

Definition

A conversation security protocol protects the security and privacy of the exchanged messages.

Conversation Security

Definition

A conversation security protocol protects the security and privacy of the exchanged messages.

This encompasses how messages are encrypted, what data is attached to them, and what cryptographic protocols (e.g., ephemeral key exchanges) are performed. A conversation security scheme does not specify a trust establishment scheme nor define how transmitted data reaches the recipient.

Conversation Security

Desirable Security and Privacy properties

- *Confidentiality* : Only the intended recipients are able to read a message.
- *Integrity* : No honest party will accept a message that has been modified in transit.
- *Authentication* : Each participant is able to verify that a message was sent from the claimed source.
- *Anonymity Preserving* : Any anonymity features provided by the underlying transport privacy architecture are not undermined.
- Causality Preserving: Implementations can avoid displaying a message before messages that causally precede it.
- Many more...it is easy to understand that the most important aspect of conversation security is *security*.

Conversation Security

Desirable Usability and Adoption properties

- *Out-of-Order Resilient* : If a message is delayed in transit, but eventually arrives, its contents are accessible upon arrival.
- *Dropped Message Resilient* : Messages can be decrypted without receipt of all previous messages. This is desirable for asynchronous and unreliable network services.
- *Asynchronous* : Messages can be sent securely to disconnected recipients and received upon their next connection.
- *No Additional Service* : The protocol does not require any additional servers for relaying messages or storing any kind of key material.
- *Multi-Device Support* : A user can participate in the conversation using multiple devices at once. Each device must be able to send and receive messages. Ideally, all devices have identical views of the conversation.

Trusted central servers (baseline)

- Requires a central server to relay messages.
- Point-to-point connection between user and server, using TLS.

Trusted central servers (baseline)

- Requires a central server to relay messages.
- Point-to-point connection between user and server, using TLS.
- Commonly adopted due to its high usability.
- Doesn't provide end-to-end confidentiality.
- Provides all repudiation features, because there isn't any cryptographic proof.

Authenticated Diffie-Hellman

- Initializing conversation with an authenticated Diffie-Hellman key exchange.
- Long-term keys used to authenticate the exchange of ephemeral keys.

Conversation Security

Evaluation

Authenticated Diffie-Hellman

- Initializing conversation with an authenticated Diffie-Hellman key exchange.
- Long-term keys used to authenticate the exchange of ephemeral keys.
- Providing confidentiality, integrity and authentication.
- Ephemeral keys ensure forward and backward secrecy.
- The message unlinkability and repudiation features are provided by using MAC keys based on the ephemeral keys.
- Further protection needed for participant consistency.

Conversation Security

Evaluation

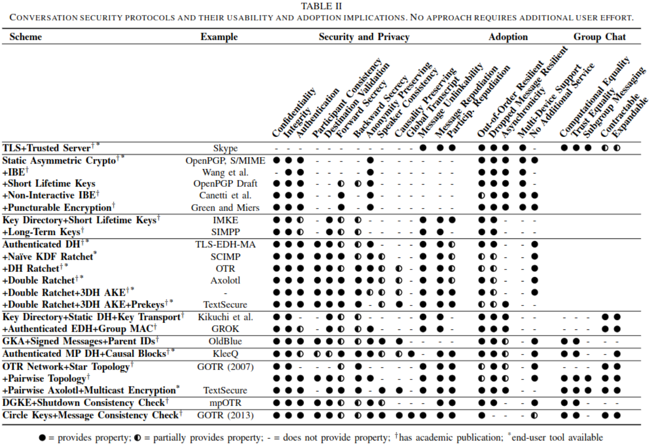

TABLE II

CONVERSATION SECURITY PROTOCOLS AND THEIR USABILITY AND ADOPTION IMPLICATIONS. NO APPROACH REQUIRES ADDITIONAL USER EFFORT.

Scheme	Example	Security and Privacy														Adoption					Group Chat				
		Confidentiality	Integrity	Authentication	Participant Consistency	Destination Validation	Forward Secrecy	Backward Secrecy	Anonymity Preserving	Speaker Consistency	Causality Preserving	Global Transcript	Message Unlinkability	Message Repudiation	Particip. Repudiation	Out-of-Order Resilient	Dropped Message Resilient	Asynchronicity	Multi-Device Support	No Additional Service	Computational Equality	Trust Equality	Subgroup Messaging	Contractable	Expandable
TLS+Trusted Server†*	Skype	-	-	-	-	-	-	-	-	-	-	-	●	●	●	●	●	●	●	-	●	●	●	◐	◐
Static Asymmetric Crypto†*	OpenPGP, S/MIME	●	●	●	-	-	-	-	●	-	-	-	-	-	-	●	●	●	●	●					
+IBE†	Wang et al.	-	●	●	-	-	-	-	●	-	-	-	-	-	-	●	●	●	●	-					
+Short Lifetime Keys	OpenPGP Draft	●	●	●	-	-	◐	◐	●	-	-	-	-	-	-	●	●	●	●	-					
+Non-Interactive IBE†	Canetti et al.	●	●	●	-	-	●	-	●	-	-	-	-	-	-	◐	●	●	●	●					
+Puncturable Encryption†	Green and Miers	●	●	●	-	-	●	-	●	-	-	-	-	-	-	●	●	●	●	●					
Key Directory+Short Lifetime Keys†	IMKE	●	●	◐	-	●	◐	◐	-	-	-	-	●	●	●	●	●	-	-	-					
+Long-Term Keys†	SIMPP	●	●	◐	-	●	◐	◐	-	-	-	-	●	●	-	●	●	-	-	-					
Authenticated DH†*	TLS-EDH-MA	●	●	●	●	●	◐	◐	●	-	-	-	●	●	◐	●	●	-	-	●					
+Naïve KDF Ratchet*	SCIMP	●	●	●	●	●	●	◐	●	◐	-	-	●	●	◐	◐	◐	-	-	●					
+DH Ratchet†*	OTR	●	●	●	●	●	◐	●	●	◐	◐	-	●	●	◐	◐	◐	-	-	●					
+Double Ratchet†*	Axolotl	●	●	●	●	●	●	●	●	◐	◐	-	●	●	◐	●	◐	-	-	●					
+Double Ratchet+3DH AKE†*	-	●	●	●	●	●	●	●	◐	◐	◐	-	●	●	●	●	◐	-	-	●					
+Double Ratchet+3DH AKE+Prekeys†*	TextSecure	●	●	●	●	●	●	●	-	◐	●	-	●	●	●	◐	◐	●	-	-					
Key Directory+Static DH+Key Transport†	Kikuchi et al.	●	●	-	-	●	◐	◐	-	-	-	-	●	●	-	●	●	●	-	-	-	-	-	●	●
+Authenticated EDH+Group MAC†	GROK	●	●	◐	-	●	◐	◐	●	-	-	-	●	●	-	●	●	●	-	-	-	-	-	●	●
GKA+Signed Messages+Parent IDs†	OldBlue	●	●	●	●	●	◐	◐	●	●	●	-	-	-	-	●	●	◐	-	●	●	●	-	-	-
Authenticated MP DH+Causal Blocks†*	KleeQ	●	●	◐	◐	◐	●	●	●	◐	◐	●	-	●	●	●	●	◐	-	●	●	●	-	-	●
OTR Network+Star Topology†	GOTR (2007)	●	●	-	-	-	◐	●	-	-	-	-	●	●	●	◐	●	◐	-	●	-	-	-	●	●
+Pairwise Topology†		●	●	●	●	●	◐	●	●	-	-	-	●	●	●	◐	●	◐	-	●	●	●	●	●	●
+Pairwise Axolotl+Multicast Encryption*	TextSecure	●	●	●	-	●	●	●	-	●	●	-	●	●	●	●	●	●	-	-	●	●	●	●	●
DGKE+Shutdown Consistency Check†	mpOTR	●	●	●	●	●	◐	◐	●	◐	-	-	-	●	●	●	●	-	-	●	●	●	-	-	-
Circle Keys+Message Consistency Check†	GOTR (2013)	●	●	●	●	●	◐	◐	●	●	●	●	●	●	●	●	-	-	-	◐	●	●	-	●	●

● = provides property; ◐ = partially provides property; - = does not provide property; †has academic publication; *end-user tool available

Figure: Evaluation of different conversation security approaches

Conversation Security

Discussion

- No conversation security protocol provides all desired properties.

Conversation Security

Discussion

- No conversation security protocol provides all desired properties.
- There is significant room for improvement by combining protocol designs.

Conversation Security

Discussion

- No conversation security protocol provides all desired properties.
- There is significant room for improvement by combining protocol designs.
- The most widely adopted solutions also have the worst security and privacy properties.

Conversation Security

Discussion

- No conversation security protocol provides all desired properties.
- There is significant room for improvement by combining protocol designs.
- The most widely adopted solutions also have the worst security and privacy properties.
- A concern that limits adoption of secure conversation security protocols is the limited support for multiple devices despite users owing multiple devices.

Transport Privacy

Definition

The transport privacy layer defines how messages are exchanged, with the goal of hiding message metadata such as the sender, receiver, and conversation to which the message belongs.

Transport Privacy

Desirable Security and Privacy properties

- *Sender Anonymity* : When a chat message is received, no non-global entities except for the sender can determine which entity produced the message.

- *Recipient Anonymity* : No non-global entities except the receiver of a chat message know which entity received it.

- *Participation Anonymity* : No non-global entities except the conversation participants can discover which set of network nodes are engaged in a conversation.

- *Unlinkability* : No non-global entities except the conversation participants can discover that two protocol messages belong to the same conversation.

- *Global Adversary Resistant* : Global adversaries cannot break the anonymity of the protocol.

Transport Privacy

Desirable Usability properties

- *No Message Drops* : Dropped messages are retransmitted.
- *No Message Delays* : No long message delays are incurred.
- *Contact Discovery* : The system provides a mechanism for discovering contact information.
- *Easy Initialization* : The user does not need to perform any significant tasks before starting to communicate.
- *No Fees Required* : The scheme does not require monetary fees to be used.

Transport Privacy

Desirable Adoption properties

- *Topology Independent* : No network topology is imposed on the conversation security or trust establishment schemes.
- *No Additional Service* : The architecture does not depend on availability of any infrastructure beyond the chat participants.
- *Low Storage Consumption* : The system does not require a large amount of storage capacity for any entity.
- *Low Computation* : The system does not require a large amount of processing power for any entity.
- Many more...Low Bandwidth , Asynchronous , Scalable

Transport Privacy

Evaluation

Store-and-Forward (baseline)

- Common for email and text messaging apps.
- Causes delays and raises the storage requirements.

Transport Privacy

Evaluation

Store-and-Forward (baseline)

- Common for email and text messaging apps.
- Causes delays and raises the storage requirements.
- Can't provide privacy properties due to headers.

Transport Privacy

Evaluation

Store-and-Forward (baseline)

- Common for email and text messaging apps.
- Causes delays and raises the storage requirements.
- Can't provide privacy properties due to headers.

Onion Routing

- Routing through multiple proxy servers, thus the message tracing is rendered difficult.

Transport Privacy

Evaluation

Store-and-Forward (baseline)

- Common for email and text messaging apps.
- Causes delays and raises the storage requirements.
- Can't provide privacy properties due to headers.

Onion Routing

- Routing through multiple proxy servers, thus the message tracing is rendered difficult.
- Latency is added, but other usability features remain unaffected.
- Sender anonymity, participant anonymity and unlinkability are provided as well.
- Global adversaries can extract information by statistical analysis methods.

Transport Privacy

Evaluation

Broadcast Systems

- Broadcast every message to ensure recipient anonymity.

Transport Privacy

Evaluation

Broadcast Systems

- Broadcast every message to ensure recipient anonymity.
- Participation anonymity and unlinkability are provided as well.

Broadcast Systems

- Broadcast every message to ensure recipient anonymity.
- Participation anonymity and unlinkability are provided as well.
- Increases the bandwidth requirements and can't support asynchronicity.

Transport Privacy

Evaluation

Broadcast Systems

- Broadcast every message to ensure recipient anonymity.
- Participation anonymity and unlinkability are provided as well.
- Increases the bandwidth requirements and can't support asynchronicity.
- Attackers can exploit flooding to disrupt the availability.

Transport Privacy

Evaluation

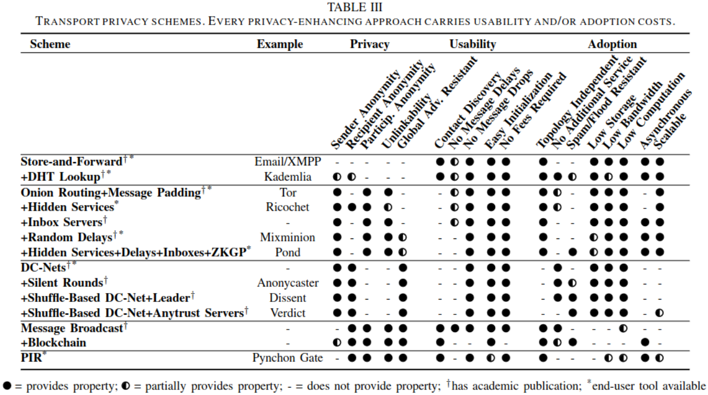

TABLE III

TRANSPORT PRIVACY SCHEMES. EVERY PRIVACY-ENHANCING APPROACH CARRIES USABILITY AND/OR ADOPTION COSTS.

Scheme	Example	Privacy					Usability					Adoption							
		Sender Anonymity	Recipient Anonymity	Particip. Anonymity	Unlinkability	Global Adv. Resistant	Contact Discovery	No Message Delays	No Message Drops	Easy Initialization	No Fees Required	Topology Independent	No Additional Service	Spam/Flood Resistant	Low Storage	Low Bandwidth	Low Computation	Asynchronous	Scalable
Store-and-Forward†*	Email/XMPP	-	-	-	-	-	●	◐	●	●	●	●	-	-	●	●	●	●	●
+DHT Lookup†*	Kademlia	◐	◐	-	-	-	●	◐	●	●	●	●	●	◐	●	◐	●	●	●
Onion Routing+Message Padding†*	Tor	●	-	●	●	-	-	◐	●	●	●	●	◐	-	●	●	●	-	●
+Hidden Services*	Ricochet	●	●	●	◐	-	-	◐	●	●	●	●	◐	-	●	●	●	-	●
+Inbox Servers†	-	●	-	●	●	-	-	◐	●	●	●	●	-	-	●	●	●	●	●
+Random Delays†*	Mixminion	●	-	●	●	◐	-	-	●	●	●	●	-	-	◐	●	●	●	●
+Hidden Services+Delays+Inboxes+ZKGP*	Pond	●	-	●	●	◐	-	-	●	●	●	●	-	●	◐	●	●	●	●
DC-Nets†*	-	●	●	-	-	●	-	-	●	●	●	-	●	-	●	●	●	-	-
+Silent Rounds†	Anonycaster	●	●	-	-	●	-	-	●	●	●	-	●	◐	●	●	●	-	-
+Shuffle-Based DC-Net+Leader†	Dissent	●	●	-	-	●	-	-	●	●	●	-	●	●	●	●	●	-	-
+Shuffle-Based DC-Net+Anytrust Servers†	Verdict	●	●	-	-	●	-	-	●	●	●	-	-	●	●	●	●	-	◐
Message Broadcast†	-	-	●	●	●	●	●	●	●	●	●	●	●	-	-	-	◐	-	-
+Blockchain	-	◐	●	●	●	●	●	-	-	●	-	●	◐	●	-	-	-	●	-
PIR*	Pynchon Gate	-	●	●	●	●	●	-	●	◐	●	●	-	-	-	◐	◐	●	◐

● = provides property; ◐ = partially provides property; - = does not provide property; †has academic publication; *end-user tool available

Figure: Evaluation of different transport privacy approaches

Transport Privacy

Discussion

- If messages are secured end-to-end, then metadata is easily hidden from service operators.

Transport Privacy

Discussion

- If messages are secured end-to-end, then metadata is easily hidden from service operators.
- Assuming that each message is sent using new channels, an adversary is not able to link single messages to conversations.

Transport Privacy

Discussion

- If messages are secured end-to-end, then metadata is easily hidden from service operators.
- Assuming that each message is sent using new channels, an adversary is not able to link single messages to conversations.
- Decentralized schemes either exhibit synchronicity issues or have serious scalability problems.

Transport Privacy

Discussion

- If messages are secured end-to-end, then metadata is easily hidden from service operators.
- Assuming that each message is sent using new channels, an adversary is not able to link single messages to conversations.
- Decentralized schemes either exhibit synchronicity issues or have serious scalability problems.
- Broadcast-based schemes can achieve the best privacy properties, but exhibit serious usability issues, such as lost or delayed messages, in addition to apparently intractable scalability issues.

Conclusions

- The vast majority of the world's electronic communication still runs over legacy protocols none of which were designed with end-to-end security in mind.

Conclusions

- The vast majority of the world's electronic communication still runs over legacy protocols none of which were designed with end-to-end security in mind.
- Since the main purpose of communication networks is to connect a large number of users, there needs to be a small amount of trustworthy protocols developed and a-la-carte systems should be avoided.

Conclusions

- The vast majority of the world's electronic communication still runs over legacy protocols none of which were designed with end-to-end security in mind.
- Since the main purpose of communication networks is to connect a large number of users, there needs to be a small amount of trustworthy protocols developed and a-la-carte systems should be avoided.
- Most of the exciting progress being made right now is by protocols that are either completely proprietary (e.g., Apple iMessage) or are open- source but lack a rigorously specified protocol to facilitate interoperable implementations (e.g., TextSecure).

Conclusions

- The vast majority of the world's electronic communication still runs over legacy protocols none of which were designed with end-to-end security in mind.
- Since the main purpose of communication networks is to connect a large number of users, there needs to be a small amount of trustworthy protocols developed and a-la-carte systems should be avoided.
- Most of the exciting progress being made right now is by protocols that are either completely proprietary (e.g., Apple iMessage) or are open- source but lack a rigorously specified protocol to facilitate interoperable implementations (e.g., TextSecure).
- A message from the authors : We have uncovered many open challenges and interesting problems to be solved by the research community. The active development of secure messaging tools offers a huge potential to provide real-world benefits to millions; we hope this paper can serve as an inspiration and a basis for this important goal.