ΕΘΝΙΚΟ ΜΕΤΣΟΒΙΟ ΠΟΛΥΤΕΧΝΕΙΟ

ΣΧΟΛΗ ΗΛΕΚΤΡΟΛΟΓΩΝ ΜΗΧΑΝΙΚΩΝ ΚΑΙ ΜΗΧΑΝΙΚΩΝ ΥΠΟΛΟΓΙΣΤΩΝ

ΥΠΟΛΟΓΙΣΤΙΚΗ ΚΡΥΠΤΟΓΡΑΦΙΑ

9ο ΕΞΑΜΗΝΟ

Παρουσίαση του

SoK: Secure Messaging

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

Γεώργιος Γκοτζιάς

Δημήτριος Κόγιος

21 Μαρτίου 2024

I. Εισαγωγή

Οι πρόσφατες αποκαλύψεις σχετικά με τη μαζική επιτήρηση από ευφυείς υπηρεσίες έχουν αναδείξει την ανάγκη για βελτίωση της ασφάλειας και της ιδιωτικότητας που προσφέρουν οι υπηρεσίες ανταλλαγής μηνυμάτων. Παρατηρείται ότι παρά την εκτεταμένη βιβλιογραφία, νέα εργαλεία αδυνατούν να ενσωματώσουν την υπάρχουσα γνώση επαναλαμβάνοντας λάθη του παρελθόντος. Αυτό οφείλεται στο ότι δεν υπάρχει κοινός στόχος, οπότε κάθε λύση στοχεύει σε συγκεκριμένο στόχο, με αποτέλεσμα να καταλήγει σε αμφισβητούμενα επίπεδα ασφάλειας.

Ο στόχος της παρούσας εργασίας είναι να ορίσει ενιαία κριτήρια, με βάση τα οποία θα αξιολογούνται οι εφαρμογές, τα οποία θα λαμβάνουν υπόψιν εκτός της ασφάλειας και χαρακτηριστικά σχετικά με την πρακτικότητα της λύσης. Γι’ αυτόν τον λόγο δίνονται ορισμοί για συγκεκριμένα χαρακτηριστικά ασφάλειας και ιδιωτικότητας, αξιολογούνται με συστηματικό τρόπο διάφορες προσεγγίσεις, είτε πρόκειται για ακαδημαϊκά τεκμηριωμένες λύσεις είτε για εφαρμογές που παρατηρούνται στην πράξη, συγκρίνονται οι αξιολογήσεις που προκύπτουν και αναδεικνύονται τα θέματα που πρέπει να εξεταστούν μελλοντικά.

II. Μεθοδολογία συστηματοποίησης

Για την αξιολόγηση των εφαρμογών διαχωρίζεται το πρόβλημα της ασφάλειας σε τρία διαφορετικά προβλήματα, τα οποία είναι σχεδόν ανεξάρτητα μεταξύ τους. Το πρώτο πρόβλημα που αξιολογείται είναι αυτό της εγκαθίδρυσης εμπιστοσύνης (από εδώ και στο εξής θα αναφέρεται ως Trust establishment), το οποίο αφορά τη διανομή των κλειδιών και την αυθεντικοποίηση των χρηστών. Στη συνέχεια, εξετάζεται το πρόβλημα της ασφάλειας της συζήτησης (conversation security), που σχετίζεται με την προστασία των ανταλλασσόμενων μηνυμάτων και τέλος το πρόβλημα της ιδιωτικότητας μεταφοράς (transport privacy), το οποίο σχετίζεται με τα μεταδεδομένα που μπορούν να εξαχθούν κατά τη μεταφορά των μηνυμάτων.

Σχετικά με την ασφάλεια, οι πιθανοί αντίπαλοι μπορούν να είναι είτε τοπικοί (ελέγχουν το τοπικό δίκτυο), είτε παγκόσμιοι (ελέγχουν μεγάλο τμήμα του διαδικτύου) είτε οι πάροχοι της υπηρεσίας.

Η μεθοδολογία της αξιολόγησης που ακολουθείται αρχικά ορίζει για κάθε πρόβλημα ποια είναι τα χαρακτηριστικά σχετικά με την ασφάλεια, τη χρηστικότητα και την ευκολία να υιοθετηθεί η αντίστοιχη λύση στην πράξη και στη συνέχεια περιγράφονται διάφορες προσεγγίσεις για την επίλυση του εκάστοτε προβλήματος. Έπειτα, για κάθε προσέγγιση περιγράφονται ποια χαρακτηριστικά υλοποιούνται και ποια όχι, ενώ προτείνονται και βελτιώσεις που θα μπορούσαν να προσφέρουν κάποια επιπλέον χαρακτηριστικά. Τα αποτελέσματα της αξιολόγσης συγκεντρώνονται σε έναν πίνακα για κάθε περιοχή, όπου κάθε στήλη αντιστοιχεί σε ένα χαρακτηριστικό και κάθε γραμμή σε μία προσέγγιση επίλυσης. Σημειώνεται ότι η αντιπροσωπευτική μέθοδος επίλυσης πιθανώς να μην προσφέρει όλα τα χαρακτηριστικά που σημειώνονται.

Σχετικά με τα χαρακτηριστικά που αξιολογούνται διακρίνονται σε τρεις κατηγορίες. Η πρώτη αφορά την ασφάλεια, δηλαδή τις αρχές της κρυπογραφίας που έχουν επιλεχθεί και το κατά πόσο σωστά έχουν υλοποιηθεί. Σε αυτή την περίπτωση δεν ελέγχεται αν υπάρχουν κάποια κενά ασφαλείας που έχουν στην πράξη εφαρμογές, παρά μόνο αν λανθασμένοι χειρισμοί από τον χρήστη μπορούν να οδηγήσουν σε παράκαμψη της ασφάλειας. Έπειτα, αξιολογείται η χρηστικότητα της λύσης, δηλαδή η ευκολία ο τελικός χρήστης να κατανοήσει πως λειτουργεί το σύστημα και οι προσπάθεια που χρειάζεται να καταβάλλει, ώστε να χρησιμοποιηθεί σωστά. Τέλος, εξετάζεται και η ευκολία να ενσωματωθεί στην πράξη η αντίστοιχη προσέγγιση, δηλαδή οι απαιτήσεις που δημιουργούνται από την αντίστοιχη λύση σε πόρους και υποδομές. Γι’ αυτόν τον λόγο συγκρίνονται οι απαιτήσεις μιας λύσης σε σχέση μία απλή λύση που χρησιμοποίειται ως αναφορά και δεν παρέχει κανένα χαρακτηριστικό ασφάλειας ή ιδιωτικότητας.

III. Trust Establishment

Πρόκειται για τη διαδικασία που οι χρήστες ανταλλάσσουν τα μακροχρόνια κλειδιά τους, καθώς και την αυθεντικοποίηση αυτών, δηλαδή την επιβεβαίωση ότι το κλειδί αντιστοιχεί στην σωστή οντότητα στην πραγματικότητα.

Σχετικά με τα χαρακτηριστικά που εξετάζονται από την πλευρά της ασφάλειας και της ιδιωτικότητας, αυτά αφορούν την προστασία από Man-in-the-Middle(MitM) επιθέσεις από τοπικούς ή παγκόσμιους αντιπάλους (Network MitM Prevention), τις επιθέσεις MitM από τους διαχειριστές των υποδομών που χρησιμοποιούνται (Operator MitM Prevention), την ανίχνευση τέτοιων επιθέσεων (Operator MitM Detection), τη δυνατότητα ελέγχου της συμπεριφοράς του διαχειριστή (Operator Accountability), την δυνατότητα ανάκτησης ή ανανέωσης των κλειδιών που χρησιμοποιούνται (Key Revocation Possible), καθώς και τα μεταδεδομένα που εξάγονται στους υπόλοιπους χρήστες ή τους παρόχους λόγω της προσέγγισης (Privacy Preserving).

Για τη χρηστικότητα της λύσης αξιολογείται αν χρειάζεται πρόσθετη προσπάθεια από τον χρήστη για τη δημιουργία ενός κλειδιού (Automatic Key Initialization), την προσπάθεια για τη διαχείριση του κλειδιου (Low Key Maintenance), την ευκολία ανταλλαγής με νέες επαφές (Easy Key Discovery) και την αλλαγή των υπάρχοντων κλειδιών (Easy Key Recover), τη χρήση ή όχι επιπλέον καναλιών (In-band), την ανάγκη για προϋπάρχουσα σχέση (No Shared Secrets), την αποφυγή των προβλημάτων από ανανέωση κάποιου κλειδιού (Alert-less Key Renewal), την άμεση λειτουργία μετά από αλλαγή των κλειδιών, καθώς και τα σφάλματα που μπορούν να προκύψουν λόγω απροσεξίας του χρήστη (Inattentive User Resistant).

Τα χαρακτηριστικά που επηρεάζουν την ευκολία υιοθέτησης της λύσης αφορούν την υποστήριξη πολλαπλών κλειδιών (Multiple Key Support), την ανάγκη για επιπλέον υποδομές, όπως κεντρικούς server (No Service Provider Required), την ανάγκη για έλεγχο σχετικά με τις υποδομές (No Auditing Required), θέματα σχετικά με τα διαθέσιμα ονόματα των χρηστών και τη δίκαιη διανομή τους (No Name Squatting), τη δυνατότητα ασύγχρονης ανταλλαγής κλειδιού και επιβεβαίωσης αυθεντικότητας, καθώς και θέματα που αφορούν την κλιμακωσιμότητα της λύσης.

Η πρώτη προσέγγιση σχετικά με το πρόβλημα Trust establishment, η οποία εξετάζεται και χρησιμοποίειται ως αναφορά και για τις υπόλοιπες αξιολογήσεις, ονομάζεται Opportunistic Encryption. Στην περίπτωση αυτή χρησιμοποίειται κρυπτογραφημένη σύνοδος, χωρίς καμία αυθεντικοποίηση για τα κλειδιά. Ένας τρόπος υλοποίησης είναι με τη μέθοδο OTR (Off-the-record) χωρίς κάποια επιβεβαίωση για το κλειδί. Η μέθοδος αυτή παρέχει ασφάλεια από επιθέσεις από παθητικούς αντιπάλους, όμως αποτυγχάνει σε οποιαδήποτε MitM επίθεση. Ο λόγος που επιλέχθηκε αυτή η μέθοδος ως αναφορά, παρά το ότι δεν προσφέρει κανένα επιθυμητό χαρακτηριστικό ασφάλειας είναι ότι η απλότητα της λύσης οδηγεί στο να παρέχονται όλα τα επιθυμητά χαρακτηριστικά που αφορούν το usability και το adoptability.

Μια επέκταση της προηγούμενης μεθόδου αποτελεί η μέθοδος TOFU (Trust-On-First-Use), η οποία αποθηκεύει κλειδιά που έχουν ήδη χρησιμοποιηθεί. Η μέθοδος αυτή παρέχει μερική προστασία από MitM επιθέσεις, καθώς απαιτεί να απουσιάζει ο αντίπαλος κατά την αρχικοποίηση των κλειδιών. Σε σχέση με την προηγούμενη μέθοδο δεν παρέχεται το χαρακτηριστικό alert-less key renewal, καθώς είναι αδύνατη η διάκριση μεταξύ καλόβουλων αλλαγών και επιθέσεων από MitM αντιπάλους, ενώ δεν είναι δυνατή και η υποστήριξη πολλαπλών κλειδιών. Στην αυστηρή της μορφή παρέχει Inattentive User Resilience, ενώ στην όχι-αυστηρή παρέχει Easy Key Recovery, χωρίς όμως να μπορεί να παρέχει και τα δύο ταυτόχρονα.

Μια άλλη βασική μέθοδος αφορά την χρήση κρυπτογραφικών hash για την επιβεβαίωση των κλειδιών εκτός ζώνης. Από άποψη χαρακτηριστικών ασφαλείας αυτή η μέθοδος είναι η βέλτιση, καθώς παρέχονται όλα τα χαρακτηριστικά, με το Key Revocation Possible να απαιτεί την εκτός ζώνης σύνδεση μεταξύ όλων των χρηστών. Παρά την ασφάλεια που παρέχεται από τη μέθοδο, οι δυσκολίες που παρουσιάζει σχετικά με τη χρηστικότητα και την εφαρμοσιμότητα την καθιστούν δύσχρηστη και δεν χρησιμοποίειται ευρέως. Για την επιβεβαίωση αντί ολόκληρου του fingerprint μπορούν να χρησιμοποιηθούν μικρότερα strings, οπότε γίνεται λόγος για τη μέθοδο Short Authentication String, ενώ αντί για απλή επιβεβαίωση του fingerprint, μπορεί να ζητείται από

τον χρήστη να εισαχθεί ολόκληρο το fingerprint, ώστε να περιοριστούν τα σφάλματα. Τότε, γίνεται λόγος για τη μέθοδο Mandatory Verification. Επίσης, παρουσιάζεται και η παραλλαγή Secret-Based Zero-Knowledge Verification, η οποία βασίζεται στο Socialist Millionaire Protocol (SMP) και αφορά τη χρήση του πρωτοκόλλου SMP για την επιβεβαίωση ενός κοινού μυστικού, αποφεύγοντας με αυτόν τον τρόπο την ανάγκη για εκτός ζώνης επικοινωνίας.

Μια άλλη ευρέως χρησιμοποιούμενη μέθοδος είναι η Authority-based Trust, η οποία προϋποθέτει μία έμπιστη αρχή για την επιβεβαίωση των κλειδιών. Τέτοιες προσεγγίσεις λειτουργούν άριστα από πλευρά χρηστικότητας, όμως δεν προσφέρουν ασφάλεια από επιθέσεις από την κεντρική αρχή. Υλοποιήσεις της μεθόδου που βασίζονται σε Public-key directories παρέχουν τη δυνατότητα ανάκτησης παλιών κλειδιών, σε αντίθεση με σχήματα Certificate Authority, στα οποία δεν είναι πρακτική η ανάκτηση κλειδιών, όμως η ανταλλαγή των πιστοποιητικών μπορεί να γίνεται απευθείας μεταξύ των χρηστών παρέχοντας ανωνυμία. Είναι δυνατές επεκτάσεις της μεθόδου, όπως η Transparency Log, ώστε να παρέχεται επιπλέον ασφάλεια σε σχέση με την κεντρική αρχή, όμως δημιουργούνται πρακτικές δυσκολίες.

Τέλος, αξιολογείται η χρήση του Blockchain ως μεθόδου ασφαλούς επικοινωνίας. Από πλευρά ασφάλειας λειτουργεί εξαιρετικά, όμως παρουσιάζονται δυσκολίες σε θέματα όπως η ανάκτηση κλειδιού, καθώς και σημαντικά ζητήματα κλιμακωσιμότητας της λύσης. Επίσης, η ανωνυμία δημιουργεί προβλήματα στην αντιστοίχηση ονομάτων, αφού θα μπορούσαν κακόβουλοι χρήστες να δεσμεύουν πολλά εύχρηστα ονόματα, το οποίο για να αντιμετωπιστεί θα έπρεπε να αυξηθεί το κόστος δέσμευσης για όλους τους χρήστες.

Όπως παρατηρείται από τον ακόλουθο πίνακα, τα υπάρχοντα πρωτόκολλα αδυνατούν να παρέχουν ταυτόχρονα security και usability, καθιστώντας αναγκαία την επιλογή στο που θα δωθεί έμφαση. Στην πράξη, εφαρμογές που προορίζονται για ευρεία χρήση ξεκινούν με βάση το να παρέχουν τη μέγιστη δυνατή χρηστικότητα και προσπαθούν να ενσωματώσουν όσα περισσότερα χαρακτηριστικά ασφάλειας μπορούν, ενώ για συγκεκριμένες χρήσεις παρέχονται σχήματα υψηλής ασφάλειας. Σχήματα, όπως το transparency log, καθώς και σχήματα που συνδυάζουν διαφορετικά πρωτόκολλα δύναται να βελτιώσουν την ασφάλεια μεθόδων υψηλής χρηστικότητας, όμως δεν έχουν εφαρμοστεί ακόμα, ώστε να υπάρχουν επαρκή δεδομένα.

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

IV. Conversation Security

Εφόσον έχει επιλυθεί το πρόβλημα Trust Establishment, εξετάζεται η ασφάλεια και η ιδιωτικότητα των ανταλλασσόμενων μηνυμάτων. Ζητήματα σχετικά με τον τρόπο επίλυσης του Trust establishment και τον τρόπο μετάδοσης των δεδομένων δεν αφορούν το συγκεκριμένο πρόβλημα, οπότε οι λύσεις που περιγράφονται είναι ανεξάρτητες από αυτά.

Τα βασικά χαρακτηριστικά ασφάλειας και ιδιωτικότητας είναι το Confidentiality, δηλαδή μόνο οι προτιθέμενοι παραλήπτες να μπορούν να διαβάσουν το μήνυμα, και το Integrity, δηλαδή να μην γίνονται δεκτά μηνύματα που έχουν αλλοιωθεί κατά τη μετάδοση. Σημαντικά χαρακτηριστικά σχετικά με την ασφάλεια είναι το Forward secrecy, δηλαδή αν μπορεί να αποκρυπτογραφηθεί ένα προηγουμένως κρυπτογραφημένο μήνυμα, συνδυάζοντας ολα τα κλειδια, και το Backward secrecy, δηλαδή αν μπορεί να αποκρυπτογραφηθεί ένα μελλοντικό μήνυμα, αν συνδυαστούν όλα τα κλειδιά. Επίσης, στον πίνακα αξιολογούνται χαρακτηριστικά που έχουν να κάνουν με το consistencytων συμμετεχόντων από την οπτική του κάθε χρήστη, ζητήματα σχετικά με την ανωνυμία των χρηστών, καθώς και τη δυνατότητα αποκήρυξης μηνυμάτων. Ακόμη, για την περίπτωση επικοινωνίας περισσότερων χρηστών λαμβάνονται υπόψιν χαρακτηριστικά σχετικά με τον δίκαιο διαμοιρασμό του φόρτου μεταξύ των χρηστών και τις μεταβολές που μπορούν να συμβούν κατά την επικοινωνία.

Σχετικά με τη χρηστικότητα, όλες οι χρησιμοποιούμενες εφαρμογές υλοποιούν την ασφάλεια των μηνυμάτων από προεπιλογή, γι’ αυτό δεν εξετάζονται ζητήματα σχετικά με την προσπάθεια που πρέπει να καταβάλλει ο κάθε χρήστης. Ανίθετα, ελέγχονται ζητήματα, όπως η δυνατότητα λήψης μηνυμάτων εκτός σειράς (Out-of-order resilient), αν είναι δυνατή η αποκρυπτογράφηση χωρίς να έχουν ληφθεί όλα τα προηγούμενα μηνύματα (Dropped Message Resilient), η δυνατότητα ασύγχρονης επικοινωνίας, η υποστήριξη πολλαπλών συσκευών και αν απαιτείται κάποια επιπλέον υποδομή.

Η μέθοδος που χρησιμοποίειται ως αναφορά επίλυσης του συγκεκριμένου προβλήματος αναφέρεται ως Trusted central servers. Πρόκειται για τη χρήση ενός κεντρικού server, στον οποίο συνδέεται κάθε χρήστης, ο οποίος αναλαμβάνει την αναμετάδοση μηνυμάτων. Για την ασφάλεια χρησιμοποίειται κάποιο πρωτόκολλο του στρώματος μεταφοράς, όπως το TLS. Αυτή η μέθοδος χρησιμοποίειται από αρκετές δημοφιλείς εφαρμογές, λόγω της ευχρηστίας της. Όμως, δεν παρέχεται end-to-end confidentiality, που είναι βασικό ζήτημα ασφάλειας. Ακόμη, όλα τα χαρακτηριστικά σχετικά με την αποκήρυξη παρέχονται από τη συγκεκριμένη μέθοδο, αφού δεν γίνεται κάποια κρυπτογραφική απόδειξη με αυτή τη μέθοδο.

Μια άλλη απλή μέθοδος αφορά τη χρήση ασύμμετρης κρυπτογράφησης (Static Asymmetric Cryptography), όπου τα long term keys χρησιμοποιουνται για την υπογραφή και κρυπτογράφηση ζευγών κλειδιών για την ασύμμετρη κρυπτογράφηση. Ενώ καταφέρνει να παρέχει confidentiality, authentication και integrity, δεν παρέχει τη δυνατότητα αποκήρυξης. Ακόμη, η απλή προσέγγιση δεν παρέχει Forward ή Backward secrecy, οπότε προτείνονται διάφορες παραλλαγές, οι οποίες μπορεί να προσφέρουν κάποιες βελτιώσεις στη συγκεκριμένη μέθοδο από πλευρά ασφάλειας.

Ένας άλλος προτεινόμενος τρόπος για επίλυση του προβλήματος Conversation security είναι η μέθοδος Authenticated Diffie-Hellman. Η μέθοδος αυτή χρησιμοποιεί τα long ter keys για να αυθεντικοποιήσει τα εφήμερα κλειδιά που παράγονται για κάθε σύνοδο από τον κάθε χρήστη. Με τα κλειδιά αυτά γίνεται συμμετρική κρυπταγρόφηση και παράγονται MAC κλειδιά. Με το βασικό αυτό μηχανισμό παρέχονται τα χαρακτηριστικά confidentiality, integrity και authentication. Λόγω των εφήμερων κλειδιών παρέχεται forward και backward secrecy, ενώ τα MAC κλειδιά παρέχουν message unlinkability και message repudiation. Ακόμη, εφόσον έχει πραγματοποιηθεί η ανταλλαγή εφήμερων κλειδιών είναι δυνατή η ασύγχρονη ανταλλαγή μηνυμάτων, η μετάδοση εκτός σειράς και αποκρυπτογράφηση, ενώ έχουν χαθεί μηνύματα. Διάφορες παραλλαγές που βασίζονται στη συγκεκριμένη μέθοδο μπορούν να βελτιώσουν περαιτέρω κάποια ζητήματα ασφάλειας, όπως το speaker consistency.

Οι παραπάνω μέθοδοι, εκτός της αναφοράς, αφορούν την επικοινωνία μεταξύ μόνο δύο χρηστών. Επομένως, στη συνέχεια εξετάζονται κάποιες λύσεις σχετικά με την επικοινωνία για περισσότερους χρήστες και τα χαρακτηριστικά που μπορούν να προσφέρονται σε αυτή την

περίπτωση. Παρατηρείται ότι η απλή επέκταση της μεθόδου αναφοράς μπορεί να παρέχει, ολικώς ή μερικώς, όλα τα επιθυμητά χαρακτηριστικά για επικοινωνία πολλαπλών χρηστών.

Στον ακόλουθο πίνακα παρουσιάζονται συγκεντρωτικά τα αποτελέσματα διάφορων μεθόδων. Είναι εμφανές, ότι καμία μέθοδος δεν μπορεί να επιτύχει όλα τα επιθυμητά χαρακτηριστικά. Με τον συνδυασμό διάφορων μεθόδων μπορούν να παρατηρηθούν βελτιώσεις, οπότε υπάρχουν ζητήματα για έρευνα στη συγκεκριμένη περιοχή. Τέλος, οι περισσότερες χρησιμοποιούμενες λύσεις δεν λειτουργούν καλά από άποψη ασφάλειας και ιδιωτικότητας. Αυτό οφείλεται στο ότι οι πιο ασφαλείς λύσεις δεν είναι πρακτικές, καθώς δεν μπορούν να υποστηρίξουν πολλαπλές συσκευές.

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

V. Transport Privacy

Το πρόβλημα Transport Privacy αφορά τον τρόπο μετάδοσης των μηνυμάτων, με σκοπό την απόκρυψη των μεταδεδομένων κάθε μηνύματος, όπως ο αποστολέας, ο παραλήπτης ή τη συζήτηση που ανήκει.

Τα χαρακτηριστικά που αξιολογούνται από πλευρά ασφάλειας και ιδιωτικότητας είναι η ανωνυμία αποστολέα (Sender Anonymity), η ανωνυμία παραλήπτη (Recipient Anonymity), η ανωνυμία συμμετεχόντων (Participant Anonymity), η αδυναμία αναγνώρισης ότι δύο μηνύματα ανήκουν στην ίδια συζήτηση (unlinkability) και η αδυναμία παγκόσμιων αντιπάλων να σπάσουν την ανωνυμία του πρωτοκόλλου (Global Adversary Resistant).

Σχετικά με τη χρηστικότητα εξετάζεται το αν το σύστημα παρέχει έναν μηχανισμό εύρεσης των επαφών (Contact discovery), αν δεν απαιτείται σημαντική καθυστέρηση για την εφαρμογή του πρωτοκόλλου (No Message Delays), αν είναι δυνατή η επαναμετάδοση μηνυμάτων που χάθηκαν (No Message Drops), αν είναι εύκολη η αρχικοποίηση πριν την έναρξη της επικοινωνίας (Easy Initialization) και αν απαιτείται κάποιο ποσό για χρήση της υπηρεσίας (No Fees Required).

Για να εξεταστεί η ευκολία ενσωμάτωσης των λύσεων στην πράξη εξετάζεται το κατά πόσο η λύση προϋποθέτει συγκεκριμένη τοπολογία (Topology Independent), αν απαιτείται κάποια παραπάνω υποδομή πέραν των χρηστών (No additional service), η διαθεσιμότητα του συστήματος

από επιθέσεις denial-of-service (Spam/Flood resistant), οι απαιτήσεις σε χώρο αποθήκευσης (Low Storage Consumption), οι απαιτήσεις εύρους ζώνης (Low Bandwidth), οι υπολογιστικές απαιτήσεις (Low Computation), η δυνατότητα ασύγχρονης επικοινωνίας, καθώς και ζητήματα κλιμακωσιμότητας.

Ως αναφορά χρησιμοποίειται η μέθοδος store-and-forward. Πρόκειται για την περίπτωση που χρησιμοποιούνται ενδιάμεσοι server, οι οποίοι αποθηκεύουν και στη συνέχεια προωθούν τα μηνύματα. Αυτή η μέθοδος χρησιμοποίειται για email και μηνύματα κειμένου, λόγω των μικρών απαιτήσεων σε χώρο αποθήκευσης και τις ελάχιστες καθυστερήσεις που δημιουργεί. Όμως, τα στοιχεία σχετικά με τον παραλήπτη και τον αποστολέα είναι εκτεθιμένα στην επικεφαλίδα, άρα δεν παρέχεται ιδιωτικότητα.

Μια άλλη λύση είναι το Onion Routing. Με τη μέθοδο αυτή η επικοινωνία γίνεται μέσω πολλαπλών proxy servers, καθιστώντας δύσκολο το tracing από άκρο σε άκρο. Εφαρμόζει πολλαπλά στρώματα κρυπτογράφησης και κάθε server αποκρυπτογραφεί μόνο ένα στρώμα, με αποτέλεσμα να μαθαίνει μόνο τον αμέσως προηγούμενο και τον αμέσως επόμενο. Το Onion Routing διατηρεί τη χρηστικότητα της baseline μεθόδου, με εξαίρεση τις καθυστερήσεις που εισάγονται. Η μέθοδος μπορεί να επεκταθεί περαιτέρω, ώστε να είναι αδύνατο για global adversaries να εξάγουν στοιχεία, καθώς στη βασική του μορφή δεν αντιμετωπίζει επιθέσεις βασισμένες σε στατιστικές αναλύσεις. Ακόμη, περαιτέρω αλλαγές είναι απαραίτητες για την αντιμετώπιση επιθέσεων denial-of-service.

Μια τρίτη προσέγγιση αποτελεί η μέθοδος DC-nets (Dining Cryptographer networks), η οποία εκτελείται σε γύρους, όπου κάθε χρήστης είτε στέλνει ένα μήνυμα είτε όχι και στο τέλος κάθε συμμετέχων λαμβάνει το xor όλων των μηνυμάτων. Η μέθοδος αυτή παρέχει σημαντική ανωνυμία, όμως εισάγει καθυστερήσεις, δεν υποστηρίζει ασύγχρονη επικοινωνία, περιορίζει την κλιμακωσιμότητα και είναι ευάλωτο σε επιθέσεις denial-of-service.

Τέλος, μπορούν να χρησιμοποιηθούν Broadcast systems, με σκοπό τη μέγιστη ανωνυμία. Στέλνοντας ένα μήνυμα σε όλους τους υπόλοιπους είναι αδύνατο να αναγνωρίσει κάποιος τον προτιθέμενο παραλήπτη. Ακόμη, παρέχεται participation anonymity και unlinkability προς κάθε επιτιθέμενο, ενώ επιλύεται άμεσα και το ζήτημα εύρεσης των επαφών. Στα αρνητικά της μεθόδου, οι αυξημένες απαιτήσεις σε bandwidth, η αδυναμία ασύγχρονης επικοινωνίας, καθώς και η κλιμακωσιμότητα.

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

Με βάση τα παραπάνω, συμπεραίνεται ότι για ασφαλή από άκρο σε άκρο επικοινωνία, τα μεταδεδομένα μπορούν εύκολα να αποκρυφθούν από τους παρόχους. Το πρόβλημα του unlinkability μπορεί να επιλυθεί εύκολα με νέα κανάλια, όμως εγείρονται ζητήματα σχετικά με τη χρηστικότητα. Επιπρόσθετα, αποκεντρωμένα συστήματα παρέχουν ισχυρή ανωνυμία, όμως αποτρέπουν την ασύγχρονη επικοινωνία και πάσχουν από περιορισμένη κλιμακωσιμότητα. Τέλος, συστήματα που χρησιμοποιούν είναι τα βέλτιστα από πλευρά ιδιωτικότητας, όμως η υιοθέτηση τους στην πράξη δεν είναι εύκολο λόγω των απαιτήσεων σε bandwidth, της έλλειψης ασύγχρονης επικοινωνίας και της αδυναμίας κλιμακωσιμότητας.

VI. Συμπεράσματα

Η τρέχουσα κατάσταση στις ηλεκτρονικές επικοινωνίες βασίζεται στη χρήση πρωτοκόλλων τα οποία δεν έχουν σχεδιαστεί με στόχο την ασφάλεια από άκρο σε άκρο. Ακόμη, δεν παρατηρείται σημαντική αύξηση στην ακαδημαϊκή έρευνα σχετικά με την ασφάλεια, γιατί πολλά ενδιαφέροντα προβλήματα με πρακτικές προεκτάσεις παραμένουν ανεπίλυτα και ταυτόχρονα πολλά επιλυμένα προβλήματα θεωρούνται μη πρακτικά. Στην πράξη, η τρέχουσα έρευνα διεξάγεται κυρίως για πρωτόκολλα που αφορούν εμπορικές εφαρμογές (Apple iMessage) ή open-source εφαρμογές χωρίς αυστηρά θεμελιωμένα πρωτόκολλα, ώστε να διευκολύνονται διαλειτουργικές υλοποιήσεις.

Το βασικό ζητούμενο των συστημάτων επικοινωνίας είναι η αλληλεπίδραση των χρηστών, οπότε ο στόχος θα έπρεπε να είναι η ανάπτυξη λίγων αξιόπιστων πρωτοκόλλων, τα οποία θα μπορούν να χρησιμοποιηθούν ευρέως. Από τη συστηματική αξιολόγηση που διεξήγαγε η τρέχουσα εργασία είναι εμφανής η ανάγκη για τα trade-offs, όμως η προσπάθεια συνδυασμού των υπάρχοντων λύσεων μπορεί να οδηγήσει σε περαιτέρω βελτιώσεις. Τέλος, από την έρευνα αναδεικνύονται τρέχοντα ζητήματα και ενδιαφέροντα ανεπίλυτα προβλήματα, τα οποία μπορούν να κινητοποιήσουν την ερευνητική κοινότητα. Ο στόχος των συγγραφέων είναι να εμπνεύσουν και να θέσουν τη βάση για την επίλυση αυτών, καθώς η βελτίωση στην ασφάλεια των επικοινωνιών μπορεί να επωφελήσει εκατομμύρια ανθρώπους.