Κρυπτογράφηση από άκρο σε άκρο, πραγματική εξήγηση

Τι λένε οι πάροχοι όταν λένε E2EE και τι δεν λένε. Μια διδακτική εξήγηση του μηχανισμού και των ορίων του, χωρίς το διαφημιστικό περιτύλιγμα.

Για να εξηγούμαστε: Το WhatsApp λέει ότι τα μηνύματά σας είναι κρυπτογραφημένα από άκρο σε άκρο. Είναι αλήθεια — και δεν είναι αρκετό. Αν το αντίγραφο ασφαλείας πηγαίνει στο iCloud ή στο Google Drive χωρίς πρόσθετη κρυπτογράφηση, η κρυπτογράφηση σπάει στο ίδιο σας το τηλέφωνο. Η επιχειρησιακή ερώτηση δεν είναι αν είναι κρυπτογραφημένο, αλλά πού βρίσκονται τα κλειδιά.

Τι σημαίνει πραγματικά η κρυπτογράφηση

Κρυπτογράφηση ενός μηνύματος σημαίνει τη μετατροπή του σε κάτι που μοιάζει με θόρυβο για οποιονδήποτε δεν κατέχει μια συγκεκριμένη πληροφορία που ονομάζεται κλειδί. Η λειτουργία γίνεται στη συσκευή του αποστολέα και, με το σωστό κλειδί, αναιρείται στη συσκευή του παραλήπτη. Ενδιάμεσα, το μήνυμα ταξιδεύει ως μια διαδοχή από bytes χωρίς προφανή σημασία. Αυτή είναι η απλή ιδέα. Το υπόλοιπο άρθρο ασχολείται με τις λεπτομέρειες που τη μετατρέπουν, ανάλογα με την περίπτωση, σε πραγματική εγγύηση ή σε μια ετικέτα μάρκετινγκ.

Το επίθετο *από άκρο σε άκρο* —στα αγγλικά *end-to-end*, συντομογραφία E2EE— προσθέτει μια ακρίβεια. Η κρυπτογράφηση δεν γίνεται για να μπορεί ένας ενδιάμεσος διακομιστής να την διαβάσει και να την παραδώσει. Γίνεται έτσι ώστε μόνο τα δύο άκρα —η συσκευή του αποστολέα και η συσκευή του παραλήπτη— να κατέχουν το κλειδί. Οποιοσδήποτε διακομιστής από τον οποίο περνά το μήνυμα βλέπει τον θόρυβο, όχι το μήνυμα. Αυτή είναι η τεχνική διαφορά με την κρυπτογράφηση *κατά τη μεταφορά*, όπου το περιεχόμενο ταξιδεύει κρυπτογραφημένο από τον έναν διακομιστή στον επόμενο, αλλά κάθε διακομιστής από τον οποίο περνά το αποκρυπτογραφεί για να το προωθήσει, ανακτώντας προσωρινά το κείμενο σε απλή μορφή.

Το παράδοξο του κοινού μυστικού

Υπάρχει ένα προφανές πρόβλημα. Για να μπορούν δύο άτομα να κρυπτογραφούν και να αποκρυπτογραφούν μηνύματα μεταξύ τους, χρειάζονται και οι δύο το ίδιο κλειδί. Αλλά πώς συμφωνούν σε αυτό το κλειδί εάν όλα όσα στέλνουν, εξ ορισμού, περνούν από ένα κανάλι όπου κάποιος θα μπορούσε να ακούει; Η συμφωνία για το κλειδί στο ίδιο κανάλι όπου αργότερα θα το χρησιμοποιήσουν φαίνεται αδύνατη: εάν ο επιτιθέμενος το ακούσει κατά τη συμφωνία, θα μπορεί να αποκρυπτογραφήσει όλα τα επόμενα. Για δεκαετίες, η κλασική κρυπτογραφία το έλυνε αυτό με τον δύσκολο τρόπο: τα κλειδιά παραδίδονταν αυτοπροσώπως, πριν ξεκινήσει η χρήση τους, σε φυσικές συναντήσεις. Οι πρεσβευτές κουβαλούσαν χαρτοφύλακες με κλειδιά ραμμένα στην επένδυση του παλτό τους.

Στο σύγχρονο ηλεκτρονικό ταχυδρομείο, αυτή η λύση δεν κλιμακώνεται. Εάν έπρεπε να πηγαίνουμε φυσικά στο σπίτι κάθε ατόμου με το οποίο σκοπεύαμε να επικοινωνήσουμε κρυπτογραφημένα, δεν θα καταφέρναμε να μιλήσουμε με κανέναν. Η ερώτηση που τέθηκε πριν από πενήντα χρόνια από την κρυπτογραφική κοινότητα ήταν η εξής: είναι δυνατόν δύο άτομα που δεν γνωρίζονται και μοιράζονται μόνο ένα δημόσιο κανάλι να συμφωνήσουν, σε αυτό το ίδιο δημόσιο κανάλι, ένα μυστικό που κανείς που ακούει το κανάλι δεν μπορεί να γνωρίζει;

Η κομψότητα του Diffie-Hellman

Το 1976, δύο μαθηματικοί ονόματι Whitfield Diffie και Martin Hellman απέδειξαν κάτι φαινομενικά αδύνατο: ότι δύο άτομα, που μιλούν μόνο μέσω ενός δημόσιου καναλιού —ενός καναλιού όπου οποιοσδήποτε μπορεί να ακούσει όλα όσα λένε— μπορούν να συμφωνήσουν σε έναν μυστικό κωδικό πρόσβασης χωρίς κανένας ακροατής να μπορεί να τον ανακαλύψει. Ακούγεται σαν μαγεία. Δεν είναι: είναι μαθηματικά. Η ανταλλαγή κλειδιών Diffie-Hellman, όπως είναι γνωστή από τότε, είναι η βάση για σχεδόν όλη την κρυπτογραφημένη επικοινωνία στο διαδίκτυο, και μισός αιώνας εντατικής χρήσης και παγκόσμιας ακαδημαϊκής εξέτασης επιβεβαιώνουν τη στιβαρότητά της. Όποιος θέλει να δει την οπτική διαίσθηση ή τα μαθηματικά μπορεί να συνεχίσει την ανάγνωση. Όποιος προτιμά να εμπιστευτεί ότι λειτουργεί μπορεί επίσης να συνεχίσει χωρίς να χάσει τον ειρμό του άρθρου.

Για όποιον θέλει να το φανταστεί σε μια εικόνα, υπάρχει μια γνωστή αναλογία με χρώματα. Φανταστείτε ότι η Αλίκη και ο Μάνος συμφωνούν δημόσια σε ένα βασικό χρώμα —ας πούμε κίτρινο— μπροστά στα μάτια της Εύας, που τους ακούει. Ο καθένας επιλέγει ιδιωτικά ένα δεύτερο μυστικό χρώμα και αναμιγνύει το μυστικό του με το κίτρινο. Η Αλίκη παίρνει ένα ιδιαίτερο πορτοκαλί. Ο Μάνος παίρνει ένα ιδιαίτερο πράσινο. Ανταλλάσσουν τα αποτελέσματα μπροστά στα μάτια της Εύας. Τώρα ο καθένας αναμιγνύει το χρώμα που έλαβε με το δικό του μυστικό, και οι δύο φτάνουν στο ίδιο τελικό χρώμα, επειδή η σειρά των αναμίξεων δεν έχει σημασία. Η Εύα είδε το κίτρινο και τις δύο ενδιάμεσες αναμίξεις, αλλά όχι τα μυστικά. Χωρίς κάποιο από τα μυστικά δεν μπορεί να φτάσει στο τελικό χρώμα. Τα πραγματικά μαθηματικά αντικαθιστούν τα χρώματα με υψώσεις σε δυνάμεις σε ομάδες modulo ή ελλειπτικές καμπύλες, αλλά η ιδέα είναι η ίδια: το κοινό μυστικό χτίζεται δημόσια χωρίς κανένας στο κανάλι να μπορεί να το ανακατασκευάσει.

Στην αριθμητική, για όποιον προτιμά να δει τον μηχανισμό: Η Αλίκη επιλέγει έναν μυστικό αριθμό a, ο Μάνος επιλέγει το b. Ανταλλάσσουν g^a και g^b δημόσια πάνω από το κανάλι. Η Αλίκη υπολογίζει $(g^b)^a$ και ο Μάνος υπολογίζει $(g^a)^b$. Και οι δύο φτάνουν στο ίδιο g^{ab}. Η Εύα βλέπει τα

g, g^a και g^b να περνούν από το κανάλι, αλλά η ανάκτηση του a από το g^a —το λεγόμενο πρόβλημα του διακριτού λογαρίθμου— απαιτεί έναν αστρονομικό υπολογιστικό χρόνο ανώτερο από την ηλικία του σύμπαντος όταν το g επιλέγεται σε μια κατάλληλη μαθηματική ομάδα.

Για όσους θέλουν να το επαληθεύσουν με μικρούς αριθμούς. Ολόκληρη η ανταλλαγή Diffie-Hellman μπορεί να γίνει με ψηφία αρκετά μικρά ώστε οι υπολογισμοί να γίνουν με το χέρι. Όποιος προτιμά να μην ασχοληθεί με την αριθμητική μπορεί να παραλείψει αυτό το τμήμα χωρίς να χάσει τον ειρμό του άρθρου. Όποιος θέλει να δει τον μηχανισμό να λειτουργεί βήμα προς βήμα, θα τον βρει εδώ. **Οι δημόσιοι κανόνες**, που οποιοσδήποτε μπορεί να διαβάσει: ένας πρώτος αριθμός $p = 11$ (στο πραγματικό Diffie-Hellman είναι περίπου τριακοσίων ψηφίων· χρησιμοποιούμε το έντεκα για να χωρέσουν οι υπολογισμοί σε μία σελίδα), μια βάση $g = 2$, και η σύμβαση ότι όλη η αριθμητική γίνεται *modulo* p — υπολογίζουμε, διαιρούμε με το p, και κρατάμε το υπόλοιπο, σαν ένα ρολόι έντεκα θέσεων που επιστρέφει στο μηδέν όταν ξεπεράσει το δέκα. **Οι ιδιωτικές επιλογές**, μία για τον καθένα και δεν μοιράζονται ποτέ: Η Αλίκη επιλέγει $a = 4$. Ο Μάνος επιλέγει $b = 7$.

Βήμα 1. Η Αλίκη υπολογίζει $2^4 = 16$, μετά $16 \bmod 11 = \mathbf{5}$. Στέλνει το πέντε. Η Εύα το καταγράφει.

Βήμα 2. Ο Μάνος υπολογίζει $2^7 = 128$, μετά $128 \bmod 11 = \mathbf{7}$. Στέλνει το επτά. Η Εύα το καταγράφει επίσης. Μετά τις δύο αποστολές, το σημειωματάριο της Εύας περιέχει τέσσερα δεδομένα: $p = 11$, $g = 2$, A = 5, B = 7. Της λείπει ο κοινός αριθμός που η Αλίκη και ο Μάνος πρόκειται να παραγάγουν — και τον οποίο η Εύα δεν θα μπορέσει να ανακατασκευάσει.

Βήμα 3. Η Αλίκη παίρνει το επτά που της έστειλε ο Μάνος και το υψώνει στον δικό της ιδιωτικό εκθέτη $a = 4$. Για να αποφύγουμε τον χειρισμό του $7^4 = 2401$, υπολογίζεται τμηματικά εφαρμόζοντας το modulo σε κάθε βήμα:

$7^2 = 49$

$49 \bmod 11 = 5$

$7^4 = (7^2)^2 = 5^2 = 25$

$25 \bmod 11 = 3$

Η Αλίκη λαμβάνει τον αριθμό **3**.

Βήμα 4. Ο Μάνος παίρνει το πέντε που του έστειλε η Αλίκη και το υψώνει στον δικό του ιδιωτικό εκθέτη $b = 7$. Πάλι τμηματικά:

$5^2 = 25 \bmod 11 = 3$

$5^4 = (5^2)^2 = 3^2 = 9 \bmod 11 = 9$

$5^6 = 5^4 \times 5^2 = 9 \times 3 = 27 \bmod 11 = 5$

Τέλος $5^7 = 5^6 \times 5 = 5 \times 5 = 25 \bmod 11 = \mathbf{3}$.

Ο Μάνος λαμβάνει επίσης το **3**.

Και οι δύο έχουν καταλήξει στον ίδιο αριθμό, το 3, δουλεύοντας παράλληλα. Κανένας από τους δύο δεν έστειλε τον ιδιωτικό του εκθέτη σε καμία στιγμή. Η Αλίκη δεν ξέρει ότι $b = 7$. Ο Μάνος δεν ξέρει ότι $a = 4$. Ο καθένας χρησιμοποίησε τη δημόσια τιμή που έστειλε ο άλλος σε συνδυασμό με τον δικό του ιδιωτικό εκθέτη, και συναντήθηκαν στον ίδιο προορισμό. **Γιατί καταλήγουν στον ίδιο αριθμό;** Αυτό που υπολόγισε ο καθένας: Αλίκη, $(g^b)^a = 2^{7\times4} = 2^{28} \bmod 11$. Μάνος, $(g^a)^b = 2^{4\times7} = 2^{28} \bmod 11$. Είναι η ίδια ποσότητα επειδή η σειρά πολλαπλασιασμού των εκθετών δεν έχει σημασία ($7 \times 4 = 4 \times 7$). Ο καθένας έφτασε από διαφορετικό δρόμο στον ίδιο προορισμό.

Και η Εύα; Έχει στο σημειωματάριό της τα $p = 11$, $g = 2$, A = 5, B = 7, και θα ήθελε το 3. Για να το υπολογίσει θα χρειαζόταν να γνωρίζει το a ή το b — αλλά κανένα από τα δύο δεν ταξίδεψε μέσα από το κανάλι. Ο μόνος της δρόμος είναι να αναρωτηθεί: «για ποιον εκθέτη a ισχύει $2^a \bmod 11 = 5$;». Με το p τόσο μικρό, μπορεί να δοκιμάσει 0, 1, 2, 3, 4... και να το βρει σε λιγότερο από ένα λεπτό. Όμως, αντικαθιστώντας το 11 με έναν πρώτο αριθμό τριακοσίων ψηφίων, ο χώρος των πιθανών εκθετών έχει περισσότερα στοιχεία από όσα άτομα υπάρχουν στο παρατηρήσιμο σύμπαν. **Μέχρι σήμερα δεν υπάρχει κανένας αλγόριθμος γνωστός στην ανθρωπότητα που να μπορεί να διασχίσει αυτόν τον χώρο σε λιγότερο από δισεκατομμύρια χρόνια.** Αυτό είναι το λεγόμενο *πρόβλημα του διακριτού λογαρίθμου*: εύκολο προς τα εμπρός, υπολογιστικά αδύνατο προς τα πίσω. Και είναι ο λόγος που η κρυπτογράφηση αντέχει ακόμα και αν η Εύα παρακολούθησε όλη τη συνομιλία γράμμα προς γράμμα.

Τρία απλά συστατικά —αριθμητική πάνω σε ένα ρολόι, ύψωση σε δύναμη, και η αντιμεταθετική ιδιότητα του πολλαπλασιασμού ($a \cdot b = b \cdot a$) — συνδυασμένα, παράγουν ένα πρωτόκολλο από το οποίο εξαρτάται η μισή ανθρωπότητα κάθε μέρα για τις ιδιωτικές της επικοινωνίες. Κανένα από τα τρία κομμάτια, μεμονωμένα, δεν φαίνεται ξεχωριστό. Το καθοριστικό είναι η συναρμολόγησή τους.

Από το Diffie-Hellman στο πρωτόκολλο Signal

Η κρυπτογράφηση από άκρο σε άκρο που χρησιμοποιούν σήμερα οι επαγγελματικές εφαρμογές ανταλλαγής μηνυμάτων βασίζεται, σχεδόν χωρίς εξαίρεση, σε μια κομψή και ενισχυμένη έκδοση της ανταλλαγής Diffie-Hellman. Το πρωτόκολλο Signal, σχεδιασμένο από τους Trevor Perrin και Moxie Marlinspike μεταξύ 2013 και 2016, είναι το σημείο αναφοράς. Συνδυάζει δύο βασικές ιδέες. Η πρώτη, η ανταλλαγή κλειδιών σε ελλειπτικές καμπύλες (X25519), που παράγει το αρχικό κοινό μυστικό μεταξύ δύο συσκευών. Η δεύτερη, το λεγόμενο Double Ratchet — διπλή καστάνια— που ανανεώνει τα κλειδιά αυτόματα με κάθε μήνυμα, έτσι ώστε η παραβίαση της συσκευής σήμερα να μην επιτρέπει την αποκρυπτογράφηση παρελθόντων μηνυμάτων, ούτε μελλοντικών μηνυμάτων αφού έχει περιστραφεί η καστάνια.

Σε Zig, η ανταλλαγή X25519 που παράγει το κοινό μυστικό μεταξύ δύο συσκευών χωράει σε έξι γραμμές, χρησιμοποιώντας την τυπική βιβλιοθήκη:

```
const std = @import("std");
const X25519 = std.crypto.dh.X25519;

// Alicia y Bruno generan cada uno un par (privada, pública).
const par_alicia = X25519.KeyPair.generate(io);
const par_bruno  = X25519.KeyPair.generate(io);

// Cada parte recibe la clave pública de la otra y deriva el mismo secreto.
const secreto_alicia = X25519.scalarmult(par_alicia.secret_key, par_bruno.public_key) catch unreachable;
const secreto_bruno  = X25519.scalarmult(par_bruno.secret_key,  par_alicia.public_key) catch unreachable;
// secreto_alicia == secreto_bruno  (32 bytes)
```

Τι συμβαίνει σε αυτές τις έξι γραμμές: Τα δημόσια κλειδιά ταξιδεύουν δημόσια. Τα ιδιωτικά κλειδιά δεν βγαίνουν ποτέ από την αντίστοιχη συσκευή. Κάθε μέρος παράγει, ξεκινώντας από το ιδιωτικό του και το δημόσιο κλειδί του άλλου, ένα ίδιο μυστικό τριάντα δύο bytes που κανείς στο κανάλι δεν μπορεί να ανακτήσει. Αυτό το μυστικό χρησιμεύει αργότερα ως σπόρος για την κρυπτογράφηση των ανταλλασσόμενων μηνυμάτων. Το Double Ratchet του πρωτοκόλλου Signal προσθέτει μια συνεχή περιστροφή αυτού του υλικού, έτσι ώστε η παραβίαση μιας στιγμής να μην θέτει σε κίνδυνο την υπόλοιπη συνομιλία.

Και τι ακριβώς υπάρχει μέσα στο `std.crypto.dh.X25519`; Καμία κρυφή μαγεία. Είναι δύο σύντομες συναρτήσεις που μπορούν να διαβαστούν ολόκληρες στην ίδια την τυπική βιβλιοθήκη της Zig. Η πρώτη παράγει το δημόσιο κλειδί από το ιδιωτικό — το «g^a» της ανταλλαγής:

```
pub fn recoverPublicKey(secret_key: [secret_length]u8) IdentityElementError![public_length]u8 {
    const q = try Curve.basePoint.clampedMul(secret_key);
    return q.toBytes();
}
```

Στη γλώσσα του άρθρου: το ιδιωτικό κλειδί «πολλαπλασιάζεται» —με την ελλειπτική έννοια, όχι τη στοιχειώδη αριθμητική— με το βασικό σημείο της καμπύλης Curve25519, και το αποτέλεσμα σειριοποιείται σε τριάντα δύο bytes. Η λειτουργία `clampedMul` είναι η ενισχυμένη έκδοση αυτού του βαθμωτού πολλαπλασιασμού: ενσωματώνει τις δικλείδες ασφαλείας που η κρυπτογραφική κοινότητα πρόσθετε με τα χρόνια για να αντισταθεί σε γνωστές οικογένειες επιθέσεων. Δύο γραμμές σώματος συνάρτησης.

Η δεύτερη συνάρτηση συνδυάζει το ιδιωτικό σας κλειδί με το δημόσιο κλειδί που σας στέλνει το άλλο μέρος. Είναι το «$(g^b)^a$» της ανταλλαγής, αυτό που παράγει το κοινό μυστικό των τριάντα δύο bytes που κανένας από τους δυο σας δεν μετέδωσε ποτέ:

```
pub fn scalarmult(secret_key: [secret_length]u8, public_key: [public_length]u8) IdentityElementError![shared_length]u8 {
    const q = try Curve.fromBytes(public_key).clampedMul(secret_key);
    return q.toBytes();
}
```

Άλλες δύο γραμμές. Το ληφθέν δημόσιο κλειδί ερμηνεύεται ως ένα σημείο πάνω στην καμπύλη και «πολλαπλασιάζεται» με το δικό μας ιδιωτικό κλειδί. Λόγω της αντιμεταθετικής ιδιότητας της πράξης της καμπύλης —ανάλογη με την αντιμεταθετική ιδιότητα του πολλαπλασιασμού των εκθετών που είδαμε στο αριθμητικό παράδειγμα— και τα δύο μέρη καταλήγουν με το ίδιο σειριοποιημένο σημείο: ακριβώς το κοινό μυστικό για το οποίο μιλάει το άρθρο.

Αυτό είναι όλο. Αυτό που σε μια εφαρμογή μοιάζει με μαγεία είναι, στην πραγματικότητα, δύο συναρτήσεις από τρεις γραμμές η καθεμία. Η τεχνική πολυπλοκότητα συγκεντρώνεται σε μία μόνο λειτουργία, την `clampedMul`, η οποία είναι γραμμένη παρακάτω στην ίδια τυπική βιβλιοθήκη, έχει ελεγχθεί για δεκαετίες από τη διεθνή κρυπτογραφική κοινότητα και είναι διαθέσιμη σε όποιον θέλει να τη διαβάσει γράμμα προς γράμμα. Δεν υπάρχει μαύρο κουτί ούτε στην εφαρμογή μας ούτε στην τυπική βιβλιοθήκη της Zig. Υπάρχει ανοιχτός κώδικας που μπορεί να καταλάβει ένας άνθρωπος, επιλέγοντας τον ρυθμό με τον οποίο θέλει να εισχωρήσει σε αυτόν.

Τι προστατεύει η κρυπτογράφηση από άκρο σε άκρο

Αυτό που προστατεύει καλά το E2EE, υποθέτοντας μια σωστή υλοποίηση, είναι το περιεχόμενο του μηνύματος κατά τη μεταφορά. Ένας ενδιάμεσος διακομιστής που λαμβάνει και προωθεί τα κρυπτογραφημένα δεδομένα θα δει μια διαδοχή ακατανόητων bytes. Ένας επιτιθέμενος με πρόσβαση στο καλώδιο, στο router, στο wifi access point θα δει το ίδιο. Ένας πάροχος υπηρεσιών που διατηρεί αντίγραφα της κίνησης δεν θα μπορεί να τα διαβάσει εκ των υστέρων. Μια κυβέρνηση που διατάζει τον πάροχο της υπηρεσίας να παραδώσει το περιεχόμενο θα λάβει τα ίδια ακατανόητα bytes που είχε ο διακομιστής εξαρχής.

Αυτό, σε πρακτικούς όρους, είναι πολλά. Είναι η διαφορά μεταξύ του να γράφεις ένα γράμμα μέσα σε έναν αδιαφανή φάκελο και να το γράφεις σε μια καρτ ποστάλ. Και τα δύο φτάνουν. Μόνο το ένα διαφυλάσσει το περιεχόμενο απέναντι στον ταχυδρόμο.

Τι δεν προστατεύει η κρυπτογράφηση από άκρο σε άκρο

Αξίζει να το γνωρίζετε εξίσου καλά. Το E2EE δεν προστατεύει τα μεταδεδομένα: ο διακομιστής εξακολουθεί να γνωρίζει ότι ο χρήστης A στέλνει δεδομένα στον χρήστη B, τι ώρα, με τι συχνότητα και από πού, παρόλο που δεν γνωρίζει τι λέει. Αυτά τα μεταδεδομένα, όπως έχουμε ήδη υποστηρίξει στο *Το να κρυπτογραφείς δεν σημαίνει ότι είσαι ιδιωτικός*, είναι συχνά πιο αποκαλυπτικά από το περιεχόμενο. Το να γνωρίζεις ότι κάποιος κάλεσε ένα δικηγορικό γραφείο εξειδικευμένο στα διαζύγια μια Παρασκευή στις 22:00 για τριάντα λεπτά αφηγείται μια ιστορία που το περιεχόμενο της κλήσης δεν αφηγήθηκε ποτέ. Είναι η ίδια κατάσταση με το να βλέπεις ένα άτομο να μπαίνει και να βγαίνει αρκετές φορές από μια ογκολογική κλινική: δεν χρειάζεται να ακούσεις τίποτα από όσα λέγονται μέσα για να φανταστείς τι συμβαίνει. Ένα μόνο μεμονωμένο

μεταδεδομένο μπορεί να μην σημαίνει τίποτα. Πολλά διασταυρούμενα μεταξύ τους σχεδιάζουν κάτι υπερβολικά παρόμοιο με την αλήθεια. Το E2EE δεν προστατεύει τα άκρα: εάν η συσκευή του παραλήπτη έχει παραβιαστεί από ένα κακόβουλο πρόγραμμα, το μήνυμα αποκρυπτογραφείται κανονικά για αυτόν τον παραλήπτη και το κακόβουλο πρόγραμμα το διαβάζει. Το E2EE δεν προστατεύει από την ταυτότητα του ίδιου του συνομιλητή: εάν η Αλίκη πιστεύει ότι μιλάει με τον Μάνο αλλά ένας επιτιθέμενος έχει παρεμβληθεί στην αρχή (ένας *man in the middle*) και το πρωτόκολλο δεν περιλαμβάνει ανεξάρτητη επαλήθευση, τα δύο μέρη καταλήγουν να μιλούν με τον εισβολέα νομίζοντας ότι μιλούν μεταξύ τους.

Υπάρχει ένα τέταρτο πράγμα που αξίζει να διατυπωθεί χωρίς ασάφεια. Το E2EE δεν εμποδίζει έναν πάροχο που ισχυρίζεται ότι το προσφέρει να κρατά, επιπλέον, ένα αντίγραφο του μηνύματος χωρίς κρυπτογράφηση στα δικά του συστήματα. Ο ισχυρισμός «τα μηνύματά μου είναι κρυπτογραφημένα από άκρο σε άκρο» και ο ισχυρισμός «ο πάροχος δεν διατηρεί το περιεχόμενό μου» δεν είναι ο ίδιος. Μια εφαρμογή μπορεί να τηρεί τον πρώτο ενώ παραβιάζει τον δεύτερο. Το έχουμε δει σε τίτλους ειδήσεων επανειλημμένα από το 2018. Ο χρήστης, εκτός εάν ο κώδικας του πελάτη είναι επαληθεύσιμος, δεν έχει τεχνικό τρόπο να διακρίνει τη μια περίπτωση από την άλλη χωρίς εξειδικευμένη έρευνα. Η πιο γνωστή περίπτωση στο ευρύ κοινό: το WhatsApp κρυπτογραφεί τα μηνύματα από άκρο σε άκρο κατά τη μεταφορά, αλλά εάν ο χρήστης ενεργοποιήσει το αντίγραφο ασφαλείας στο iCloud ή στο Google Drive χωρίς πρόσθετη κρυπτογράφηση, αυτό το αντίγραφο αποθηκεύεται αναγνώσιμο σε υποδομή τρίτου, και η κρυπτογράφηση σπάει στο άκρο του ίδιου του χρήστη.

Η ερώτηση που ο πάροχος δεν θέλει να ακούσει

Μια εφαρμογή που ισχυρίζεται ότι κρυπτογραφεί από άκρο σε άκρο μπορεί, τεχνικά, να κάνει ένα από τρία πράγματα όσον αφορά τα κλειδιά:

1. **Τα κλειδιά βρίσκονται μόνο στις συσκευές.** Παράγονται και βρίσκονται αποκλειστικά στις συσκευές των χρηστών. Ο πάροχος δεν τα γνωρίζει ούτε τα αποθηκεύει. Αυτή είναι η βέλτιστη περίπτωση.
2. **Ο πάροχος μπορεί να έχει πρόσβαση αν το θέλει.** Ο πάροχος έχει τα κλειδιά των χρηστών (ή μπορεί να τα δημιουργήσει κατά βούληση) και τα φυλάσσει στις βάσεις δεδομένων του. Εάν το θέλει ή εξαναγκαστεί, μπορεί να διαβάσει το περιεχόμενο. Αυτή είναι η περίπτωση των περισσότερων υπηρεσιών «cloud».
3. **Ο πάροχος δεν μπορεί να έχει πρόσβαση βάσει σχεδιασμού, αλλά ελέγχει την πρόσβαση.** Ο πάροχος δεν έχει τα κλειδιά, αλλά έχει τον έλεγχο της εφαρμογής που τα δημιουργεί. Εάν εξαναγκαστεί, μπορεί να στείλει μια κακόβουλη ενημέρωση που θα υποκλέψει τα κλειδιά ή το περιεχόμενο πριν από την κρυπτογράφηση. Αυτή είναι η περίπτωση πολλών εμπορικών υπηρεσιών E2EE.

Η επιχειρησιακή ερώτηση, επομένως, δεν είναι αν κάτι είναι κρυπτογραφημένο, αλλά ποιος έχει τον έλεγχο της συσκευής και του λογισμικού που διαχειρίζεται τα κλειδιά. Στο Solo2, τα κλειδιά βρίσκονται αποκλειστικά στη «Θυρίδα» σας (κρυπτογραφημένη IndexedDB με τον κωδικό σας) και το λογισμικό είναι επαληθεύσιμος ανοιχτός κώδικας.

Για τον επαγγελματία αναγνώστη

Η κρυπτογράφηση από άκρο σε άκρο είναι ένα εργαλείο ψηφιακής κυριαρχίας. Αλλά όπως κάθε εργαλείο, η αποτελεσματικότητά του εξαρτάται από το χέρι που το κρατά και το έδαφος στο οποίο στηρίζεται.

1. Πού παράγονται τα κρυπτογραφικά κλειδιά και πού βρίσκονται φυσικά; Εάν ο πάροχος μπορεί να έχει πρόσβαση σε αυτά (έστω και προσωρινά, έστω και υπό τη μορφή ανάκτησης), το E2EE είναι μόνο ονομαστικό.
2. Υπάρχει ανεξάρτητη επαλήθευση του συνομιλητή (αριθμοί ασφαλείας, κωδικοί QR, σύγκριση εκτός καναλιού) που να αποτρέπει μια επίθεση man-in-the-middle κατά την εγκαθίδρυση της συνομιλίας;
3. Είναι ο κώδικας του πελάτη ελέγξιμος —ανοιχτός, δημοσιευμένος, αναπαραγώγιμος— ή απαιτεί να εμπιστευτούμε τον λόγο του παρόχου για το τι πραγματικά κάνει ο πελάτης;
4. Τι μεταδεδομένα παράγει και διατηρεί η υπηρεσία, και για πόσο καιρό; Ακόμη και αν το περιεχόμενο είναι αδιαφανές, τα μεταδεδομένα μπορούν να ανακατασκευάσουν μεγάλο μέρος των ευαίσθητων πληροφοριών.

Αυτές οι τέσσερις ερωτήσεις δεν ζητούν προηγμένες τεχνικές πληροφορίες. Ζητούν πληροφορίες που κάθε έντιμος πάροχος μπορεί να απαντήσει στη δημόσια τεκμηρίωσή του. Η ποιότητα και η ακρίβεια της απάντησης λέει τόσα πολλά για το προϊόν όσα και η ίδια η απάντηση.

Η κρυπτογράφηση από άκρο σε άκρο, όταν γίνεται σωστά, είναι μια από τις πιο λεπτές κατασκευές που η σύγχρονη κρυπτογραφία έχει προσφέρει στην καθημερινή πρακτική. Η αρχική ιδέα —δύο άτομα να μπορούν να συμφωνήσουν σε ένα μυστικό μέσω ενός δημόσιου καναλιού— ανήκει στους Whitfield Diffie και Martin Hellman, 1976. Μισό αιώνα αργότερα συνεχίζουμε να ζούμε με τις συνέπειές της. Όμως, όπως συμβαίνει με κάθε τεχνική υπόσχεση, η αξία της εξαρτάται από την πραγματική συμμόρφωση, όχι από την ετικέτα. Η ερώτηση του έντιμου επαγγελματία δεν είναι «είναι κρυπτογραφημένο;», αλλά «ποιος έχει τα κλειδιά;». Οι απαντήσεις έχουν διαφορετικές συνέπειες. Αξίζει να τις γνωρίζετε.

Πηγές και περαιτέρω μελέτη

- Diffie, W.· Hellman, M. — *New Directions in Cryptography*, IEEE Transactions on Information Theory, Νοέμβριος 1976. Θεμελιώδες άρθρο της κρυπτογραφίας δημόσιου κλειδιού.
- Perrin, T.· Marlinspike, M. — *The Double Ratchet Algorithm*, δημόσια προδιαγραφή της Open Whisper Systems, αναθεώρηση 2016. Βάση του πρωτοκόλλου Signal και των βιομηχανικών του παραγώγων.
- RFC 7748 — Elliptic Curves for Security (IETF, Ιανουάριος 2016). Κανονιστική προδιαγραφή των καμπυλών X25519 και X448 που χρησιμοποιούνται στις σύγχρονες ανταλλαγές κλειδιών.
- Ferguson, N.· Schneier, B.· Kohno, T. — *Cryptography Engineering: Design Principles and Practical Applications* (Wiley, 2010). Κεφάλαια για την ανταλλαγή κλειδιών και τα πρωτόκολλα πιστοποιημένης κρυπτογράφησης.

- Κανονισμός (ΕΕ) 2024/1183 για το ευρωπαϊκό πλαίσιο ψηφιακής ταυτότητας (eIDAS 2) — καθιερώνει πλαίσια όπου η ανεξάρτητη επαλήθευση του συνομιλητή αποκτά θεσμική υποστήριξη, και όπου η διάκριση μεταξύ ονομαστικής και πραγματικής κρυπτογράφησης έχει διαφορετικές νομικές συνέπειες.

← ΠροηγούμενοKill switch και θεσμική αιχμαλωσίαΕπόμενο →Το επιχειρηματικό μοντέλο ως σήμα εμπιστοσύνης

Πρόσφατα αναγνώσματα

- Ανάλυση · 18 Μαΐου 2026 Πραγματική vs φαινομενική ιδιωτικότητα: οι ερωτήσεις που πρέπει να θέσετε
- Ανάλυση · 18 Μαΐου 2026 Self-hosting ως επαγγελματική πρακτική
- Έννοια · 18 Μαΐου 2026 Οι 24 λέξεις: τι είναι μια κρυπτογραφική ταυτότητα

Πάρτε αυτό το άρθρο μαζί σας όπου το χρειάζεστε.

↓ Markdown ↓ Απλό κείμενο ↓ PDF

Το αρχείο θα ληφθεί στη συσκευή σας. Από εκεί μπορείτε να το αποθηκεύσετε, να το εισαγάγετε στο Solo2 ή να το μοιραστείτε όπου θέλετε. Το Cuadernos δεν αποφασίζει τον προορισμό για εσάς.

Σφραγίδα από βουλοκέρι · SHA-256 a04cc928c020ac5360d2a1da4b2fa3dfd3bae1d7704dc874be61f03b01da549f

Cuadernos Lacre · Μια έκδοση της Menzuri Gestión S.L. ·
γραμμένη από τον R.Eugenio · επιμελημένη από την ομάδα του Solo2.