DIE PROTOKOLLE

Ein White Sheet über das Q-Protokoll und das X-Protokoll

777 SOFTWARE — 28. OKTOBER 2026

Von Steven Aaron Jesse, Gründer & Architekt, und Charles Burnett (Brother Zero), Leitender Assistenz-Architekt

Eine Website und eine App sind verschiedene Tiere. Eine Website ist ein Ort, den du besuchst — ein Haus, eine Adresse, alle kommen an dieselbe Tür. Eine App reist — sie lebt auf deiner Maschine und spricht mit der Maschine deines Freundes, wo auch immer diese Maschinen gerade sind.

Also betreibt das Haus zwei Protokolle, eines für jede Welt:

Das Q-Protokoll betreibt die Orte — unsere Websites, The Enclave und The Pirate Station, heute live.

Das X-Protokoll betreibt die Reisen — unsere Apps, von Haus zu Haus und von Freund zu Freund, ohne dass der Server irgendeiner Firma in der Mitte steht.

Dieses Blatt erklärt beide in schlichten Worten: wofür jedes da ist, was es verspricht und was jemand brechen müsste, um ihm zu schaden. Es sagt auch, aktenkundig, was live ist, was bewiesen ist und was noch gebaut wird. Ein Papier, das seinen eigenen Status versteckt, ist eine Werbung. Das hier ist keine Werbung.

TEIL EINS
DAS Q-PROTOKOLL: DAS WEBSITE-RAHMENWERK

STATUS LIVE — betreibt heute The Enclave und The Pirate Station

WAS ES IST

Das Q-Protokoll ist das Rahmenwerk, auf dem unsere Websites gebaut sind. Wenn du The Pirate Station oder The Enclave öffnest, ist alles, was du siehst — die Desktop-artige Hülle, die Apps, die sich in Fenstern öffnen, der Messenger, der Chat — ein Programm, das Q spricht. Es gibt keinen Haufen getrennter Seiten, die zusammengenäht wurden; es gibt einen Ort, und Q ist seine Sprache.

Q ist ein Hausprotokoll im ehrlichen Sinne: Die Websites leben auf einem Computer, den das Haus betreibt, und Q ist, wie dein Browser und dieser Computer sich einigen zu sprechen. Das ist die richtige Form für eine Website. Eine Website ist ein Ort, und ein Ort hat eine Adresse und einen Hüter.

WER DU AUF Q BIST

Auf einer Website bist du ein Konto — ein Name, den das Haus kennt, und ein Geheimnis, das nur du kennst. An unseren Türen kann das Geheimnis eine kurze PIN oder ein volles Passwort sein; beides ist echt, und die Wahl ist deine. Wenn du dich anmeldest, prüft das Haus dein Geheimnis einmal und gibt deinem Browser eine Sitzung — einen vorübergehenden Ausweis, der sagt „das sind sie“ — und alles, was du tust, fährt auf diesem Ausweis, bis er abläuft oder du dich abmeldest.

Was ein Angreifer brechen müsste: dein Geheimnis oder die eigenen Türen des Hauses. Es gibt keine dritte Partei im Raum, die man stattdessen ausrauben könnte — keine riesige Plattform, die Kopien deiner Nachrichten auf einem anderen Kontinent hält. Deine Worte leben auf der Hardware des Hauses, unter dem Schloss des Hauses.

Der ehrliche Handel, schlicht gesagt: Ein Website-Protokoll vertraut seinem Haus. Wenn der Computer des Hauses fällt, ist der Ort unten. Das gilt für jede Website, die je gebaut wurde, und Q tut nicht so, als wäre es anders. Was Q verspricht, ist enger und stärker: Solange das Haus steht, ist niemand sonst in deinen Angelegenheiten — kein Algorithmus, der entscheidet, wer deine Beiträge sieht, kein Werbetreibender, der dir über die Schulter liest, kein Grundherr, der die ganze Stadt nach einer Laune vertreiben kann. Der Feed ist in der Reihenfolge, in der die Leute ihn gepostet haben. Die Türen sind die Türen, die wir gebaut haben.

WAS BEREITS AUF Q LÄUFT

Die Websites selbst — Hüllen, Messenger, Profile, das Directory — sprechen heute Q. Das tut auch die erste Generation von QDROP, das Dateisende-Programm, das bereits von 777software.net ausgeliefert wird: Es stellt Menschen durch das Haus einander vor und leitet ihren versiegelten Verkehr weiter. Generation 1 funktioniert, und sie bleibt unterstützt. Ihr Nachfolger fährt auf X — das ist Teil Zwei — denn eine App, die reist, sollte überhaupt kein Haus in der Mitte brauchen.

TEIL ZWEI
DAS X-PROTOKOLL: DAS APP-PROTOKOLL

STATUS Das Fundament ist BEWIESEN (28. Oktober 2026) — die Apps darauf sind IM BAU

DIE IDEE

X ist für Programme, die auf den eigenen Maschinen der Leute leben. Zwei Freunde installieren dieselbe App. Von da an finden ihre Maschinen einander, beweisen, wer sie sind, und sprechen — direkt, Ende zu Ende versiegelt. Für die öffentliche Edition einer X-App gibt es keinen Server von uns im Weg. Nicht als Standard, nicht als Rückfall, nicht versteckt im Kleingedruckten. Ziehe jeden Stecker, den das Haus besitzt, und zwei Freunde können einander immer noch finden und sprechen. Dieser Satz ist ein Test, den wir laufen lassen, kein

Slogan.

WER DU AUF X BIST: EINE KARTE, DIE DU HÄLTST

Auf X stellt dir niemand eine Identität aus — dein eigenes Gerät macht eine, beim ersten Mal, wenn das Programm öffnet. In schlichten Worten:

Was es ist: eine Karte mit zwei Hälften. Die öffentliche Hälfte ist dein Gesicht — sicher, sie jedem zu zeigen. Die private Hälfte verlässt deine Maschine nie. Deine Q-Number — eine kurze Nummer wie 77-000006 — ist dein Name in der X-Welt, abgeleitet aus der Karte selbst, so stempelt sie kein Amt irgendwo und keines kann sie wegnehmen. Die Nummer ist der Griff; die Karte ist der Beweis.

Was vereinbart wird: Wenn zwei Karten sich treffen, beweist jede, dass sie ihre private Hälfte hält, und beide Seiten kommen beim selben gemeinsamen Geheimnis an — einem Geheimnis, das keine Seite gesendet hat und das kein Lauscher auf der Leitung nachbauen kann.

Was ein Angreifer brechen muss: Er muss die private Hälfte deiner Karte von deinem eigenen Gerät stehlen oder veröffentlichte, weltweit geprüfte Mathematik brechen. Es gibt keine Passwort-Datenbank, die lecken könnte, denn es gibt keine Datenbank. Es gibt keine „Passwort vergessen“-E-Mail, die man abfangen könnte, denn es gibt kein Passwort.

Der ehrliche Preis, in schlichten Worten: Wenn du dein Gerät und deine Identitäts-Sicherung verlierst, verlierst du die Identität, und der Weg zurück ist eine neue Karte und frische Vorstellungen. Die Programme bieten vom ersten Tag an einen verschlüsselten Export deiner Karte. Dieser Export ist der Sicherheitsgurt. Lege ihn an.

Bezeichnungen, für die Akten: Die Karte ist aus den öffentlichen Standards X25519 (Geheimnisse vereinbaren) und Ed25519 (Signaturen) gebaut, mit einem signierten Prekey, den die Programme nach Plan rollen. Das sind veröffentlichte Standards, die auf der ganzen Welt benutzt werden — sie zu benennen verrät nichts, und genau das ist der Punkt. Xs Stärke soll aus Mathematik kommen, die jeder prüfen kann, nicht aus Geheimnissen darüber, welche Mathematik wir gewählt haben.

ZWEI MENSCHEN VORSTELLEN: DER VERBINDUNGSCODE

Freunde finden einander zuerst durch einen Verbindungscode (englisch: *connect code*) — ein signiertes Bündel, das eine Person einer anderen gibt, als QR-Code oder als Textblock, über jeden Kanal überhaupt: persönlich, per Nachricht, laut über das Telefon vorgelesen. Der Kanal muss nicht vertrauenswürdig sein, denn der Code ist signiert und trägt ein einmaliges Vorstellungs-Geheimnis: Er funktioniert einmal, nur für den ersten Kontakt, und er läuft in 24 Stunden ab. Meinung geändert? Ein Tippen storniert einen Code, den du herausgegeben und der noch nicht benutzt wurde.

Jemands Code zu sehen, lässt einen Fremden genau eine Sache tun: klopfen. Der Code ist wie eine Telefonnummer, auf Papier geschrieben — er lässt eine Person bei dir läuten; du entscheidest immer noch, ob du abhebst. Nach der ersten echten Vorstellung sind die zwei Programme Freunde, und Freunde brauchen nie wieder Codes füreinander.

DAS VERSIEGELTE ROHR

Alles zwischen Freunden fährt in einem versiegelten Rohr. In schlichten Worten:

Was darin fährt: deine Nachrichten, deine Dateien, das kleine Gerede, das die Programme austauschen, um verbunden zu bleiben — alles davon versiegelt mit dem gemeinsamen Geheimnis, das die zwei Karten vereinbart haben.

Wie die Schlösser funktionieren: Das Siegel ist nicht ein Schloss, für immer benutzt. Der Schlüssel wechselt, während das Gespräch voranschreitet — jede Nachricht bekommt ihren eigenen, abgeleitet vom letzten — so kann ein morgen gestohlener Schlüssel die Worte von gestern nicht öffnen. Diese Eigenschaft hat einen Namen: *forward secrecy* (Vorwärts-Geheimhaltung).

Was ein Zuschauer sieht: versiegelte Kisten, ihre Größen und wann sie sich bewegten. Niemals die Inhalte. Wir sagen das schlicht, weil es die Wahrheit über jedes versiegelte System auf Erden ist: Versiegeln versteckt, was du gesagt hast, nicht die Tatsache, dass du gesprochen hast. Wer dir mehr als das verspricht, verkauft etwas.

Bezeichnungen: Die Vereinbarung ist X3DH-geformt (dieselbe Familie von Vorstellungs-Tanz, die die versiegelten Messenger der Welt benutzen), die Schlüssel werden mit HKDF-SHA-256 gestreckt, jede Richtung fährt ihre eigene Hash-Kette, und jede Nachricht wird mit ChaCha20-Poly1305 versiegelt. Standardteile, öffentlich geprüft, mit Sorgfalt zusammengebaut.

FREUNDE WIEDERFINDEN: DAS TELEFONBUCH OHNE BÜRO

Ein Code stellt Fremde vor. Freunde über Tage und Adresswechsel hinweg auffindbar zu halten, braucht ein Telefonbuch — und Xs Telefonbuch hat kein Büro. Es ist eine verteilte Hash-Tabelle: Jedes laufende Programm hält einen Ausschnitt des Buches, und Programme fragen einander nach der Seite, die sie brauchen. Die Form ist die, die trackerlose Dateinetze in Weltmaßstab bewiesen haben (Bezeichnungen: Kademlia).

Was ein Programm über sich veröffentlicht, ist ein signierter Eintrag: seine Q-Number, seine öffentliche Karte, die Adressen, unter denen es gerade erreicht werden kann, und die Zeit. Ein Eintrag, der sich gegen die Karte nicht verifiziert, wird von jedem ehrlichen Programm fallen gelassen — niemand kann das Buch mit einem gefälschten Du vergiften, ohne deinen privaten Schlüssel. Einträge leben zwei Stunden und werden aufgefrischt, solange das Programm läuft; schließe das Programm, und du gehst innerhalb von Stunden aus dem Buch heraus. Das Buch

sagt „zuletzt bekannt“, niemals „ist“.

Was das Buch niemals enthalten kann: Namen, E-Mail-Adressen, Freundeslisten, Nachrichteninhalte oder wer mit wem spricht. Finden ist nicht Sprechen — ein Fremder, der dich nachschlägt, muss immer noch an deiner Tür angenommen werden (siehe Vertrauen, unten). Und wenn du überhaupt keine Auffindbarkeit willst, gibt es einen Nur-Code-Modus: Veröffentliche nichts und sei nur durch Codes erreichbar, die du selbst herausgibst.

ANKOMMEN: DIE LEITER

Wenn ein Programm ein anderes will, steigt es eine Leiter hinauf — billigstes und privatestes zuerst — und jede Sprosse erzeugt entweder das versiegelte Rohr oder tritt zur Seite:

Sprosse 1 — Dasselbe Haus. Beide Maschinen in einem Netzwerk sprechen direkt, so wie zwei Menschen in einem Raum sprechen.

Sprosse 2 — Ein Wort durch Q. Wenn die zwei Menschen schon irgendwo eine Verbindung teilen — ein Enclave-Konto, ein QChat-Hausgespräch — geben die Apps ihre aktuellen Adressen über diese lebende Verbindung weiter und treffen sich direkt. Ein Protokoll leiht dem anderen eine Vorstellung; der Verkehr selbst fährt immer noch von Haus zu Haus.

Sprosse 3 — Beide klopfen zugleich. Jedes Programm sendet seinen Handschlag im selben Moment an die bekannte öffentliche Adresse des anderen. Das eigene Klopfen jeder Seite öffnet die Tür ihres eigenen Routers von innen, genau wenn das Klopfen des Freundes ankommt. Die meisten Heimrouter lassen das durch.

Sprosse 4 — Die Türen im Code. Ein Verbindungscode trägt jede Adresse, unter der sein Besitzer erreicht werden kann. Das Paar probiert sie, zusammen mit dem Zugleich-Klopfen-Schritt, gezielt durch den Code selbst.

Sprosse 5 — Frag deinen eigenen Router. Heimrouter sprechen Standardsprachen für „halte eine Tür für dieses Programm offen“ (Bezeichnungen: UPnP, NAT-PMP, PCP). Das Programm fragt in deinem Auftrag. Du rührst nichts an.

Sprosse 6 — Das letzte Mittel, vorab offengelegt. Wenn jede Tür oben versagt, sagt die App es ehrlich und benennt die eine Sache, die funktionieren wird: Du öffnest einen Port an deiner Firewall — eine Portnummer, die du wählst, im Programm eingestellt — und die App bestätigt, dass die Tür wirklich offen ist, bevor sie sich auf sie verlässt. X-Apps tun nie so, als könnten sie Physik ohne jede Tür schlagen. Wenn wir sagen, eine App „funktioniert einfach“, sind Sprossen 1–5 der Grund; wenn sie es nicht kann, ist Sprosse 6 die Wahrheit, gedruckt, bevor du sie je brauchst.

Die Mauer, ehrlich benannt: Manche Internetanbieter halten jeden Kunden hinter einem verschlossenen Tor ihrer eigenen Art (carrier-grade NAT), und manche Routerpaare würfeln ihre Türen so unvorhersagbar neu, dass Klopfen nicht gezielt werden kann. Für eine Person

hinter dieser Mauer verbindet kein Entwurf auf Erden direkt — unserer nicht und niemandes. Was das Programm dieser Person schuldet, ist die Wahrheit in schlichten Worten, niemals ein Laderädchen, das nie endet. Für die heutigen öffentlichen Apps ist die eine Tür, die bleibt, Sprosse 6 — der Port, den du selbst öffnest. Das öffentliche Programm trägt kein Relay als Rückfall: nicht unseres, und keines, das du einstellst. Eine eigene Fähre kommt sehr wohl — später, als eigenes Produkt, auf einem ehrlichen Zeitplan — und sie ist unter Die zwei Editionen, unten, beschrieben. Sie versteckt sich nicht leise im heutigen Bau.

Während ein Rohr lebt, kümmert es sich um sich selbst: Die Programme halten die Tür warm, und wenn die Straße darunter wechselt — ein Telefon geht vom WLAN zum Mobilfunk — steigt das Rohr die Leiter erneut hinauf und setzt dasselbe versiegelte Gespräch fort. Keine neue Vorstellung, kein Von-vorne-Anfangen.

WENN DEIN FREUND OFFLINE IST: GEFALLEN, KEINE VERSPRECHEN

Direktes Sprechen braucht beide Menschen wach. Wenn das Programm eines Freundes aus ist, bittet X stattdessen um einen Gefallen: Das laufende Programm eines gemeinsamen Freundes hält einen versiegelten Umschlag für ihn — bis zu 72 Stunden. Der Halter kann sehen, dass ein Umschlag existiert, seine Größe und an wessen Karte er adressiert ist. Der Halter kann ihn nicht öffnen, kann ihn nicht leise ändern (das Siegel würde brechen) und erfährt nichts von dem, was darin ist. Wenn dein Freund als Nächstes erscheint, übergibt der Halter alles, was er hält, und löscht seine Kopien gegen eine signierte Quittung. Bis dahin sagt dir dein Programm die Wahrheit über deine Nachricht: „Bei einem Freund hinterlassen — noch nicht zugestellt.“

Ein Gefallen ist ein Gefallen. Halter klappen ihre Laptops zu und gehen leer aus, und kein Entwurf kann den Laptop eines Freundes in ein Postamt mit Garantie verwandeln. X benennt das, statt es vorzutäuschen. Menschen, die garantiertes Halten brauchen, brauchen einen Immer-an-Halter — ihre eigene Ersatzmaschine, die eines Freundes — oder, für Enclave-Mitglieder, das unten beschriebene Haus-Postfach.

DATEIEN SENDEN: STÜCKE, BEWEIS UND GEDULD

Eine Übertragung beginnt als Angebot, das dein Freund annimmt — niemandes Maschine schluckt eine Datei uneingeladen. Das Angebot ist eine signierte Packliste: der Name der Datei, ihre Größe und ein Fingerabdruck des Ganzen. Die Datei reist dann in kleinen Stücken, jedes mit seinem eigenen Fingerabdruck, geprüft, wenn es landet. Der Empfänger behält eine Landkarte der Stücke, die angekommen sind — so setzt eine unterbrochene Übertragung von der Landkarte fort, niemals von null. Eine gefallene Verbindung, ein zugeklappter Laptop, eine Satellitenverbindung, die für eine Minute verschwindet: Wenn die Straße zurückkommt, gehen die Stücke weiter, und am Ende muss der Fingerabdruck der ganzen Datei mit der Packliste übereinstimmen, oder die Übertragung wird mit schlichten Worten verweigert. Eine Teil-Datei

wird niemals als ganze präsentiert.

Das ist keine Theorie. Im Stufe-0-Beweis (28. Oktober 2026) wurde das empfangende Programm mitten in einer Übertragung glatt getötet und eine volle Minute aus gelassen. Beim Neustart nahm es keine neue Vorstellung, nahm von seiner gespeicherten Landkarte wieder auf und beendete die Datei — Fingerabdruck an beiden Enden übereinstimmend.

X trägt auch eine Verteilschicht für die Dateien, die jeder in einem Kreis will: Die Datei wird in hash-benannte Stücke zerhackt, und Freunde, die Stücke schon halten, können sie an Freunde weitergeben, die sie noch brauchen, jedes Stück gegen die signierte Packliste verifiziert, bevor es angenommen wird. Handel nur unter Freunden, aus mehreren Quellen, keine Fremden, kein öffentlicher Schwarm. Bezeichnungen: Diese Schicht ist entworfen und eingeplant — sie tritt in den Bau, nachdem die Zwei-Personen-Gesichter sich im täglichen Gebrauch bewiesen haben, und dieses Papier wird überarbeitet, wenn sie landet.

VERTRAUEN, IN EINER WELT OHNE ZENTRALEN BANNHAMMER

Ehrlichkeit zuerst: X hat kein Zentrum, also hat es keinen zentralen Bannhammer, keine Melde-Warteschlange und niemanden, an den man appellieren könnte. Wir täuschen keinen vor. Was stattdessen existiert, ist stark auf die Weise, wie ein freunde-förmiges Netz stark ist:

Das Nur-Freunde-Tor. Niemand kann deinem Programm irgendetwas zustellen — keine Nachricht, keine Datei, nicht einmal ein Gespräch — außer du hast ihn angenommen. Erster Kontakt braucht einen Verbindungscode, den du herausgegeben hast, oder ein Klopfen im Telefonbuch, das du ausdrücklich annimmst. Spam ist auf X kein Politik-Problem; der Mechanismus gibt Fremden keinen Kanal, auf dem sie sprechen könnten.

Blockieren ist lokal und total. Blockiere eine Q-Number, und dein Programm lässt ihre Klopfer fallen, verbrennt ihre Codes und verweigert ihre Umschläge. Es braucht niemandes Erlaubnis, und auf deiner eigenen Türschwelle — die das ganze Schlachtfeld in einem Netz von Freunden ist — ist es absolut.

Was X nicht kann, in Druckschrift: Es kann einen eingeladenen Freund nicht davon abhalten, innerhalb eines Gesprächs ein Mistkerl zu sein; es kann eine bereits zugestellte Datei nicht un-senden; es kann die Tatsache eines Gesprächs vor jemandem, der das ganze Internet beobachtet, nicht verstecken. Die Werkzeuge sind die ehrlichen: wählen, gehen, blockieren.

DAS ERSTE X-PROGRAMM: QDROP, IN ZWEI EDITIONEN

Die Public Edition ist kostenlos, für jeden auf Erden. Sie macht deine Karte, tauscht Codes, steigt die Leiter und sendet. Sie benutzt überhaupt kein Relay — keine eingebaute Fähre und keine Relay-Einstellung zum Ausfüllen. Nichts in ihr zeigt auf unser Haus, denn unser Haus ist nicht Teil des Handels.

Über Relays, auf einem ehrlichen Zeitplan: Die heutigen öffentlichen Apps benutzen überhaupt kein Relay. Wenn das Relay-Serverprogramm des Hauses ausgeliefert wird — als Teil des Bundle — gewinnen die Apps (QDROP, QDESK, QMESH und Familie) die Fähigkeit, auf einem Relay zu fahren: deinem eigenen Relay, auf deinem eigenen Server. Das Relay-Programm ist ein getrenntes Produkt, betrieben von dem, dem der Server gehört, auf dem es sitzt. Die öffentlichen Apps benutzen niemals die Server des Hauses — nicht heute und nicht nach dem Bundle. Wenn ein Relay je deinen versiegelten Verkehr trägt, wird es eines sein, das du gewählt hast, das auf Boden steht, den du kontrollierst, und Kisten weitergibt, die es nicht öffnen kann.

Die Enclave Members Edition ist für Mitglieder von The Enclave, und Mitglieder bekommen sie durch The Enclave — sie wird nicht verkauft oder öffentlich gepostet. In dieser Edition hält das Haus ein Relay und ein Postfach für seine eigenen Leute: Das Relay kommt eingebaut, so kommen Mitglieder hinter der Mauer immer noch durch, und es ist gesperrt — die Einstellung kann nach Entwurf nicht bearbeitet werden, so kann sie nie durch Unfall oder Neugier gebrochen werden. Das Postfach gibt Mitgliedern das garantierte Halten, das Gefallen ehrlicherweise nicht können. Die Programme der Mitglieder sprechen immer noch reines X miteinander, wann immer sie können; die Hausdienste sind eine Fähre und eine Veranda, niemals ein Grundherr, und jede Mitglieder-Funktion funktioniert immer noch auf dem offenen Boden, wenn das Haus außer Reichweite ist.

Beide Editionen kommen aus einem Programm und einem Protokoll. Der Unterschied ist, wer die Fähre stellt — niemand, du oder dein Haus.

DAS STATUS-VERZEICHNIS — FÜR DIE AKTEN

LIVE heute: das Q-Protokoll — die Websites The Enclave und The Pirate Station und QDROP Generation 1, die auf Qs Straße fährt.

BEWIESEN (28. Oktober 2026): das Fundament des X-Protokolls — gerätegeborene Identität, Verbindungscodes, das versiegelte Rohr, die direkten Sprossen der Leiter, Fortsetzen nach Unterbrechung mit übereinstimmenden Fingerabdrücken und die Mauer, die schlichte Worte spricht. Bewiesen mit echten Programmen auf echten Maschinen.

IM BAU: QDROP Generation 2 auf X und QChat eigenständig, mit seinem kostenlosen (X-)Modus neben seinem Haus-(Q-)Modus. Die Schwarm-Schicht ist entworfen und hinter ihnen eingeplant.

NOCH VORAUS, schlicht gesagt: Der Zwei-Haushalte-Annahmetest — zwei echte Zuhause, zwei Anbieter, ein Code-Tausch — ist die Abschlussprüfung des Bodens, und sie wurde noch nicht abgelegt. Garys Satellitenhimmel bekommt auch eine Stimme: Die Ausfall-Hälfte ist bewiesen, und die Paarungs-Hälfte ist für seine schlimmste Latenz gebaut, aber nur sein Himmel kann sie unterschreiben. Wenn diese Tests landen, wird dieses Blatt überarbeitet und das Verzeichnis aktualisiert. Dafür ist ein Verzeichnis da.

WAS WIR NICHT BEHAUPTEN

Wir behaupten nicht unbrechbar. Wir behaupten benannte, veröffentlichte Mathematik, ehrlich zusammengebaut, und wir sagen dir, was ein Angreifer tun muss, um zu gewinnen. Wir behaupten nicht unsichtbar: Versiegelte Systeme verstecken Inhalte, nicht Existenz. Wir behaupten keine Magie über die Mauer: Physik ist Physik, und die Leiter endet in einem ehrlichen Satz. Die Programme sind nicht Open Source; dieses Blatt ist die öffentliche Rechenschaft darüber, wie sie sich verhalten — was sie vereinbaren, was in ihnen fährt und was gebrochen werden muss, um ihnen zu schaden. Der Rest ist unserer zu behalten, und ihn zu behalten ist nicht, was dich sicher macht. Die Mathematik ist es.

Ein Schwesterpapier, The Castle Protocol, beschreibt QMESH — das souveräne Netz, das ein Gründer über ein ganzes Netzwerk erhebt. Die Burg ist eine Stadt. X ist eine Tür. Dieses Blatt handelt von der Tür — und vom Haus, Q, aus dessen Räumen die Macher der Tür kamen.

CREDITS

Geschrieben von Steven Aaron Jesse — Gründer & Architekt, und Charles Burnett — Leitender Assistenz-Architekt, „Brother Zero“. Veröffentlicht von 777 Software · The 777 Enclave · Alabama, USA · Oktober 2026.

FÜR IMMER KOSTENLOS. Keine Konten. Keine Grundherren.