Zeitschrift: Saiten : Ostschweizer Kulturmagazin
Herausgeber: Verein Saiten
Band: 21 (2014)
Heft: 238

Artikel: "Gelöscht ist nicht weg"
Autor: Riedener, Corinne
DOI: https://doi.org/10.5169/seals-884547

«Gelöscht ist nicht weg»

Der Threema-Gründer und gebürtige Ostschweizer Manuel Kasper über Kryptografie, das virtuelle Briefgeheimnis und Medienkompetenz. *von Corinne Riedener*

Was bist du, Kryptograf? Mathematiker? Nerd?

Manuel Kasper: Ich bin Informatiker, aber Kryptografie hat mich schon immer fasziniert. Allerdings verstehe ich die aktuellen Verfahren auch nicht bis ins letzte Detail, da die heutige Kryptografie ja hohe Mathematik ist. Leute, die fähig sind, solche Algorithmen zu entwickeln, sind deshalb meistens beides, Mathematiker und Kryptografen.

Ron Rivest, Miterfinder des verbreiteten RSA-Kryptosystems, gilt als Koryphäe und geht auf die siebzig zu. Gibt es keine jungen Cracks?

Schwer zu beurteilen. RSA wurde wie viele Algorithmen, die heute eingesetzt werden, bereits in den 80ern patentiert und ist immer noch aktuell. Wenn man nicht gerade ein Genie ist, braucht man wohl schon ein bestimmtes Alter, oder zumindest die Erfahrung, um so etwas hervorzubringen – was natürlich nicht heisst, dass Junge keine neuen Algorithmen kreieren.

Nach deiner Informatiklehre hast du gleich noch ein Studium angehängt. War Kryptografie ein grosses Thema damals, Anfang der Nullerjahre?

Es hatte sicher noch nicht denselben Stellenwert wie heute, aber wir hatten schon verwandte Module, diskrete Mathematik zum Beispiel, die nützlich waren, um die Kenntnisse zu vertiefen.

2011, als du die ersten Pläne für Threema geschmiedet hast, setzte sich Daniel Ellsberg für WikiLeaks ein, Julian Assange sass in London, Edward Snowden noch für die NSA in Japan. Was bewog dich dazu, einen Krypto-Messenger zu entwickeln?

Ich war unzufrieden mit dem Status quo: SMS waren kostenpflichtig und das Handynetz ohnehin nicht sehr gut geschützt. Die Alternative, der WhatsApp-Messenger, war wiederum extrem offen. Praktisch jeder konnte mitlesen. Adressbuchdaten, Chatprotokolle oder Benutzerprofile waren nicht nur für die Mobilfunkanbieter einsehbar, sondern für alle mit dem nötigen Equipment – obwohl viele Verschlüsselungs-Algorithmen ja bereits seit Jahren existierten. Für mich ging es vor allem darum, diese mit einem möglichst simplen Messenger zu verschmelzen. Bedienungsfreundlichkeit, das war die Grundidee. Als Apple wenig später die verschlüsselten iMessages auf den Markt brachte, habe ich meine Pläne allerdings wieder auf Eis gelegt. Ein Jahr später habe ich sie wieder hervorgeholt und eher zum Spass begonnen, eine iOS-Applikation zu entwickeln. Nachdem sie den Test in meinem Kollegenkreis bestanden hatte, habe ich sie Ende 2012 kostenlos in den App-Store gestellt und staunte nicht schlecht, als sie innerhalb von wenigen Stunden bereits einige tausend Downloads verzeichnete. Nach 10'000 wurde der Preis auf zwei Franken festgelegt.

Und dann kam Snowden.

Die erste grosse Welle – innert Tagen hat sich die Nutzerzahl verzehnfacht.

Im vergangenen Februar, als WhatsApp an Facebook verkauft wurde, kam der zweite grosse Schub, drei Millionen fast über Nacht. War Sicherheit nie Thema in der IT-Szene, bevor die Snowden-Files veröffentlicht wurden?

Schon, aber es war eher eine individuelle Angelegenheit. Ich würde nicht behaupten, dass Informatiker grundsätzlich security-affin sind, wobei es natürlich immer solche mit paranoiden Zügen gab. Andererseits war es vielen erstaunlich egal, obwohl sich die Branche einig war, dass mitgelesen wird.

Sichere Verbindungen wie SSL und HTTPS gibt es seit Jahren.

Heute schaut man genauer darauf, wie man etwas verschlüsselt. Ein Web-Server mit SSL zum Beispiel: Früher hat man ihn einfach so aufgesetzt und konfiguriert, dass es funktioniert; heute achtet man darauf, nur sichere Algorithmen zu verwenden. Es gibt Webseiten, die andere diesbezüglich testen und «Walls of Shame» führen.

Threema

«Was man nicht hat, kann man nicht herausgeben», sagt Manuel Kasper auf die Frage nach den Daten der Threema-Benutzer. Seit Februar, als der Instant-Messenger WhatsApp an Facebook verkauft wurde, haben sich über drei Millionen User die Threema-App auf ihre Mobiltelefone geladen. Unterdessen hat der 30-jährige Informatiker mit zwei weiteren Software-Entwicklern eine GmbH gegründet und eine Android-App auf den Markt gebracht.

Derzeit arbeiten sie an einer Version für das Windows-Phone. Die Threema-Server stehen in Zürich. Alle Nachrichten der User werden sofort nach der Zustellung von den Servern gelöscht. Die Daten sind so verschlüsselt, dass nur der Server weiss, wer mit wem Kontakt hat, sagt Kasper, aber die Inhalte bleiben auch für die Maschine ein Geheimnis. Threema setzt wie Telegram, myEnigma und andere Krypto-Messenger auf asymmetrische Kryptografie.

Die App generiert dabei zweierlei Schlüssel bei der Installation; einen öffentlichen zum Ver- und einen privaten zum Entschlüsseln. Die Nachricht ist also nutzlos, wenn sie abgefangen wird, da sie nur mit dem Gerät des Empfängers entschlüsselt werden kann. Für die Übertragung wird die verschlüsselte Nachricht trotzdem nochmals zusätzlich verschlüsselt, sagt Kasper. Damit kein Aussenstehender weiss, von wem sie kommt und wohin sie geht.

Wie sensibilisiert man denn die Gesellschaft, wenn es die Herausforderung einer ganzen Generation ist, die Verschlüsselung an sich zu entschlüsseln – ohne Studium?

Leider kann man Netzwerke, Datentransfers und Kryptografie nicht in zwei Sätzen erklären. Bei der Entwicklung geht es deshalb vor allem darum, die Algorithmen so zu verpacken, dass sie ihren Dienst möglichst unbemerkt tun, damit sich die Nutzer nicht mit lästigen Add-Ons und Plug-Ins plagen müssen. Je komplizierter eine Anwendung ist, desto weniger wird sie genutzt.

Die technische Hemmschwelle ist demnach ziemlich hoch, trotz der Enthüllungen in den vergangenen Jahren. Was muss passieren, dass die User verstehen, dass die Überwachung auch für sie zum Problem werden könnte?

Keine Ahnung... Es gab zwar viele, die ihre Nachrichten danach eine Zeit lang verschlüsselt haben, aber kaum war die Empörung halbwegs verebbt, wurde vielfach wieder auf den Schutz verzichtet – weil es ohne eben rascher geht. Immerhin ist das Sicherheitsbewusstsein in der IT-Branche gewachsen, aber im Detail damit auseinandergesetzt haben sich wohl nur die wenigsten. Dabei gäbe es eigentlich genügend Algorithmen, wenn sie richtig eingesetzt würden.

Was ist mit Ron Rivests RC4-Algorithmus, von dem Jacob Appelbaum, Bruce Schneier und andere Experten glauben, dass ihn die NSA in Echtzeit entschlüsselt?

Dieser bald dreissigjährige Algorithmus war stets beliebt, da er äusserst effizient, platzsparend und einfach zu implementieren ist. Eigentlich wusste man spätestens, nachdem WEP, die erste Wireless-LAN-Verschlüsselung, deswegen geknackt wurde, dass RC4 nicht mehr zu empfehlen ist. Eine kurze Renaissance erlebte er 2011, als eine Sicherheitslücke im SSL-Protokoll gefunden wurde, die praktisch alle Verschlüsselungsalgorithmen ausser dem RC4 betraf – weil er eben grundsätzlich anders funktioniert. Jedenfalls haben danach einige kurzfristig wieder auf RC4 umgestellt, was sie wiederum angreifbar machte. Aber sowas kommt oft vor und hat selten mit dem Algorithmus, sondern mehr mit seiner Verwendung zu tun.

Könnte man auch zurück, zu längst veralteten Techniken?

Natürlich, auch das kommt vor. Über all den aktuellen Verfahren schwebt ja ohnehin das Damoklesschwert des Quantencomputers. Wenn man dort irgendwann genügend Quanten-Bits verbauen kann, lassen sich die meisten der derzeit verwendeten Verschlüsselungen innert Kürze knacken, selbst wenn es mit der heutigen Technologie Millionen von Jahren dauern würde.

Es geht das Gerücht, dass die NSA mit – oder zumindest an – Quantencomputern arbeitet.

In diesem Zusammenhang hört man oft von der sogenannten post-quantum cryptography: Es gibt tatsächlich auch quantencomputersichere Algorithmen. In der Praxis sind sie allerdings kaum verbreitet, weil sie zu viele Ressourcen benötigen.

Interessiert dich die «theoretische» Kryptografie?

Dafür fehlt mir einerseits der mathematische Background, andererseits ist mir das Ganze noch zu unpraktisch, da ich es ja anwenden will. Abgesehen davon relativiert sich die Sicherheit eines Verschlüsselungsverfahrens, solange die Applikation auf einem Betriebssystem oder einer Hardware läuft, die wir nicht kontrollieren...

Du sprichst von Backdoors?

So ist es. Wir wissen nicht, was sich in der Hardware und im Betriebssystem alles versteckt. Eine Applikation an sich mag vielleicht sicher sein, ob gewisse Inhalte nicht doch gespeichert oder zum Beispiel unbemerkt Screenshots gemacht werden können, ist unbekannt. Eine Software kann deshalb nie sicherer sein als die Plattform, auf der sie läuft. Und falls wirklich ein Hintertürchen eingebaut ist, kann man sowieso alles mitlesen – bevor etwas verschlüsselt wird.

Ähnlich wie die Trojaner, die im revidierten Bundesgesetz zur Überwachung des Post- und Fernmeldeverkehrs (BÜPF) vorgesehen sind, nur dass die Malware später eingeschleust wird. Wie stehst du dazu?

Mir ist klar, dass schwere Verbrechen gewisse Massnahmen erfordern, aber ich bin gegen die geplante Verschärfung. Aus idealistischen Gründen, anders als zum Beispiel

Um zu verifizieren, ob der öffentliche Schlüssel auch wirklich dem Empfänger gehört, arbeitet Threema mit einem Ampelsystem: Für grünes Licht muss man eine Person persönlich treffen und ihren Schlüssel einscannen – die sicherste Variante. Wurden Kontakte durch den freiwilligen Abgleich mit dem Telefonbuch gefunden, steht die Ampel auf orange, gänzlich unbekannte Kontakte bleiben rot. Threema arbeitet für den kryptografischen Teil mit einer Open Source Library (NaCl), der Quellcode der App selber ist aber nicht öffentlich. «Das hat vor allem wirtschaftliche Gründe», sagt Kasper, «da wir angewiesen sind auf die Einkünfte aus den App-Verkäufen, um die Weiterentwicklung zu finanzieren, die Server zu betreiben, Support zu leisten etc.» Kritische Stimmen fordern deshalb unabhängige Audits, die Threema-Entwickler zweifeln jedoch am Sinn solcher Expertisen. «Konsequenterweise müsste man dann auch jedes noch so kleine Update einzeln testen lassen. Das ist aber teuer, verzögert die Entwicklung und schadet deshalb letztlich den Nutzern», sagt Kasper. «Abgesehen davon kann man auch Open Source-Programmen erst vertrauen, wenn man den Quellcode persönlich überprüft hat.»

die Provider, die sich eher aus wirtschaftlichen Gründen wehren. Die erweiterte Vorratsdatenspeicherung wäre für sie ja mit grossen Mehrkosten verbunden.

Manche User plädieren dafür, gleich alles öffentlich zu machen.

Das hat etwas von Fatalismus, von Schwarz-weiss-Denken. Es geht ja nicht darum, dass man nichts mehr preisgibt, sondern dass man sich bewusst ist, über welchen Kanal man es tut.

Müssten wir ein Schulfach haben, um medienkompetenter zu werden?

Nützlich wäre es sicher, wobei es weniger auf das Technische ankommt, sondern eben auf den Umgang. Was kann ich bedenkenlos veröffentlichen? Was bespreche ich besser persönlich? Schliesslich wissen wir: Gelöscht ist nicht weg.

In der britischen Serie *Utopia* wird das Orwellsche Szenario ziemlich konkret weiter gesponnen: Gesichtserkennung, Suchanfragen, IP-Adressen, Krankenakten und Verbrechen – die Schattenmacht manipuliert, wo sie kann. Darf man sich davor fürchten?

Eine der grössten Ängste ist es, dass man irgendwann fähig ist, ein umfassendes Bild zu kreieren aus den Daten mehrerer Kanäle. Mit Big Data versucht man das ja bereits, aber es ist kaum abzuschätzen, wie weit diese Entwicklung wirklich ist. Was man machen kann, wird aber bekanntlich gemacht, deshalb ist es wichtig, sich für die Privatsphäre einzusetzen.

Krypto-Messenger sind auf dem Vormarsch. Was, wenn euch in einigen Jahren für die Threema-App x Milliarden geboten werden?

Bis jetzt hatten wir noch keine konkreten Angebote, aber es haben nun mal alle ihren Preis. Etwas anderes zu behaupten wäre wohl realitätsfern. Zudem fragt sich, wozu man so etwas kaufen will. Um es vom Markt zu werfen? Um es zu kontrollieren?

Oder um die Idee des virtuellen Briefgeheimisses zu schützen?

Auch das Briefgeheimnis hat Grenzen. So wie es Techniken gibt, reale Briefe unbemerkt zu lesen, gibt es auch im Netz Methoden, von denen man nie wirklich sicher ist, ob sie angewendet werden oder nicht.

Darktown

Alle überwachen das Netz – Saiten überwacht die Stadt. Das erweist sich allerdings als völlig unnötig. *von Peter Surber*

15 Uhr. Mittwochnachmittag, das Strassencafé ist voll besetzt. Kontrollblick von oben zeigt: Touristen zumeist, ältere Semester mit Fotoapparaten. Ein behelmter Velofahrer saust vorbei. Ein Durchschnittsnachmittag, und der Überwachungsjob bis jetzt: todlangweilig. Da, schon wieder ein Velo, diesmal ein bekanntes Gesicht, hallo, wir winken uns zu vom Erker hinab zur Gasse, von der Gasse hinauf zum Erker. Vor dem «Bäumli» stehen die Lieferwagen der Handwerker, die das Erdgeschoss zum Ladengeschäft umbauen. Elektro, Natursteine, Metallbau. Sie versperren den Passanten und Velos den Durchgang, unerlaubterweise. Ein Kind schreit.

Es ist eine unangenehme Rolle: Gassenüberwachung von oben herab, aus dem Pelikanerker in der Schmiedgasse, dem Redaktionsbüro von Saiten. Im Septemberheft hatte Martin Amstutz in seinem Text über Whistleblower Edward Snowden das Stichwort gegeben und Parallelen vom elektronischen Datenüberwachungsirrsinn zur alten Stadtrepublik St.Gallen gezogen: «So ein Erker ist nicht nur repräsentativ, er dient auch dazu, die Konkurrenz auszuspähen und das Wohlverhalten der Untergebenen zu überwachen.» Konkurrenz hat Saiten zwar keine, und statt «Untergebenen» sind es heutzutage bloss Untendurchgehende; Bürger, Passantinnen, Gehetzte, Schlendernde, Ziellose. Ihnen gemeinsam scheint, und der Eindruck erhärtet sich nach mehrstündiger stichprobenartiger Gassenüberwachung: alle völlig harmlos.

«Öffentliche Plätze und Strassen können mit Videokameras überwacht werden.» (Art. 3 des Polizeireglements der Stadt St.Gallen) Plakatieren ohne Bewilligung wird zum Offizialdelikt, für Demonstrationen gilt ein Vermummungsverbot, und: «Die Polizei kann vorübergehend Personen von öffentlichem Raum wegweisen oder fernhalten» (Art. 4). Präzis vor zehn Jahren, im Herbst 2004, ist im Stadtparlament dieses Polizeireglement debattiert und verabschiedet worden. Im Mai 2005 sagte die Bevölkerung nach heftigem Abstimmungskampf Ja zum Reglement, 15'437 Ja zu 8'037 Nein. Der Widerstand dagegen war grundsätzlich: Er stellte das Recht der Stadt in Frage, ihre Bewohner polizeilich zu überwachen. Die Debatte beschränkte sich nicht auf St.Gallen: Bern war 1998 schweizweit vorangegangen, St.Gallen folgte, später Luzern und die meisten anderen, auch kleinere Städte.

Zitat Saiten von damals: «Ruhe, Ordnung, Schöngeist. Die Entwicklung der zunehmenden Privatisierung des St.Galler Stadtraums gipfelt im neuen Polizeireglement. Was stört, wird weggewiesen.» Ein Jahrzehnt danach: Kein Thema mehr? Wo bleibt die Diskussion? Sie verläuft statt politisch: soziologisch.

16 Uhr. Auf dem Grüningerplatz, nicht weitab vom Erker, ist die Zeichnerin Lika Nüssli an der Arbeit. Sie pinselt mit weisser Farbe Fragen auf das Kopfsteinpflaster. Es ist eine von mehreren Stationen der diesjährigen Sozialraumta-