Ein Sieb für Algorithmen

Suche nach Quantencomputer-sicherer Kryptografie

Quantencomputer der nächsten Generation würden heute übliche asymmetrische kryptografische Schlüssel und Signaturen schnell knacken. Das gefährdet auch das weltweite Domain Name System. Es gibt zwar neue kryptografische Methoden, aber noch ist unklar, welche den essenziellen Internetdienst schützen können.

Von Monika Ermert und Dušan Živadinović

Wer das Domain Name System (DNS) kontrolliert, bestimmt, welches Ziel ein Browser nach dem Auflösen des Servernamens tatsächlich ansteuert. Das bedeutet: Wenn Angreifer Internetnutzern falsche IP-Adressen unterschieben, können sie diese in Fallen locken, um Zugangsdaten zu Onlinediensten zu erbeuten (siehe c't 7/2019, S. 52).

Deshalb werden zumindest der Startpunkt des DNS (Root-Zone) und die meisten Top-Level-Domains wie .de oder .com mittels DNS Security Extensions geschützt (DNSSEC). Dabei signiert man die im Klartext übertragenen DNS-Informationen kryptografisch (z. B. IP-Adressen). So können Empfänger per Signaturprüfung sicherstellen, dass die Daten nicht manipuliert wurden und dass sie von einer befugten Quelle kommen (c't 12/2022, S. 126). Mit Verschlüsselungen wie DNS-over-HTTPS kann man die Daten zwar ebenfalls vor Manipulation schützen, aber die Methoden sind nur für einen Teil der Strecke ausgelegt und sie eignen sich nicht, um den Absender zu authentifizieren, weshalb DNSSEC unverzichtbar ist.

Vorgetäuschte Befugnis

Doch die Signaturen gründen auf herkömmlichen Algorithmen wie RSA und ECDSA, die Attacken mit künftigen Quantencomputern wahrscheinlich nicht standhalten werden. Der Knackpunkt ist die Prüfung der Vertrauenswürdigkeit: Wer die dafür verwendeten Signaturen bricht, kann falsche, aber technisch korrekt signierte DNS-Antworten unterschieben und damit etwa Browser auf präparierte Server umleiten.

Gegen solche Angriffe sollen neue, Quantencomputer-sichere Algorithmen helfen (Post-Quantum Cryptography, PQC). Die laufende Suche nach Kandidaten koordiniert das US-amerikanische National Institute of Standards and Technology (NIST). Beispielsweise hält das NIST das TLS-Protokoll für besonders wichtig, weil viele Internetanwendungen darauf aufsetzen. Wenn Angreifer komplette Dialoge zwischen Client und Server mitschneiden, könnten sie die aktuellen TLS-Chiffren in einigen Jahren mit leistungsfähigen Quantencomputern knacken. Dagegen könnten einige vom NIST ausgewählte neue Chiffrieralgorithmen helfen (siehe ct.de/yzhd).

Offen blieb zunächst, wie gut sich diese Algorithmen für DNSSEC eignen. Um das zu untersuchen, haben Nils Wisiol, Matthieu Grillere und Peter Thomassen das Toolset PQ-DNSSEC entwickelt und auf GitHub veröffentlicht. Die EU-Kommission fördert das Projekt über den niederländischen NGI Assure Fund.

Feldtest in Sicht

Zum Toolset gehören autoritative DNS-Server und Resolver, die Signaturen neuer Algorithmen erzeugen und prüfen. Auch lässt sich damit und anhand von Beispieldatensätzen die Kompatibilität von Implementierungen mit der öffentlichen DNS-Infrastruktur prüfen. Dazu planen Wisiol und Thomassen eine Feldstudie mit diversen Algorithmen und suchen weitere Mitstreiter.

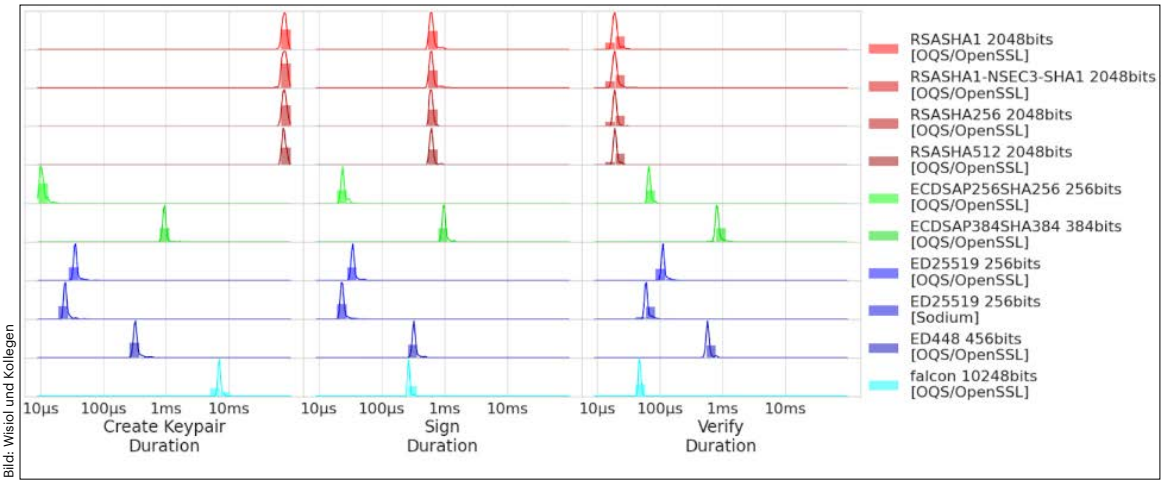

Bild: Wisiol und Kollegen

DNS-Informationen werden aktuell mit Verfahren wie RSA und ECDSA geschützt, die aber Angriffen durch Quantencomputer vermutlich nicht standhalten werden. Das neue Falcon512 schneidet leider nur in Geschwindigkeitsvergleichen gut ab.

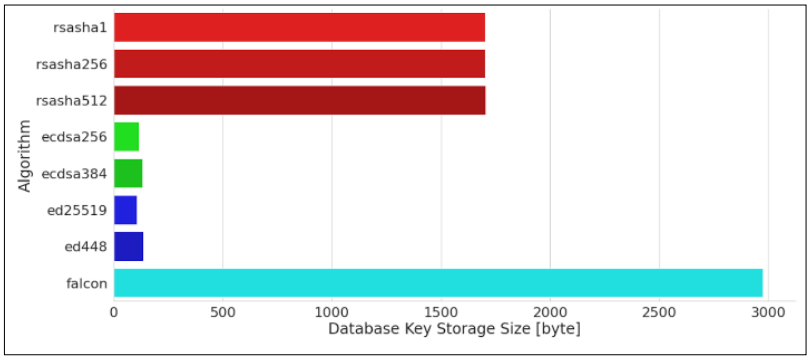

Bild: Wisiol und Kollegen

Mit Falcon512 erzeugte Signaturen belegen rund doppelt so viel Platz wie jene, die man herkömmlich per RSA erzeugt. Betreiber großer DNS-Server müssten dafür höhere Kosten in Kauf nehmen.

Bisher haben sie den Algorithmus Falcon512 untersucht, der ersten Analysen aus dem Jahr 2020 zufolge hohe Geschwindigkeit und gute Leistung liefern sollte. In ihrem Blog-Beitrag vom April 2022 stellten sie die Schlüsselerzeugung, Signierung und Validierung mit Falcon512 vor. Unterm Strich kam heraus: Schlüsselpaare und Signaturen erzeugt Falcon512 etwas schneller als das lange Zeit gängige RSA mit 2048 Bit und nur wenig langsamer als ECDSA. Bei der Validierung muss sich Falcon512 nur RSA geschlagen geben.

Sorgenkind Paketgrößen

Doch die mit Falcon512 signierten DNS-Pakete dürften zu groß sein. Die Paketgröße ist aus zwei Gründen bedeutsam: Betreiber von autoritativen DNS-Servern müssen für die signierten Daten genügend Speicherplatz bereitstellen. Je länger die Schlüssel und je mehr signierte DNS-Zonen ein autoritativer Server enthält, desto größer der Platzbedarf. Daher sehen Betreiber großer DNS-Server lange Signaturen skeptisch.

Schwerwiegender ist der zweite Grund: Für die DNS-Kommunikation wird überwiegend das schnelle User Datagram Protocol verwendet (UDP). Doch in vielen altmodisch ausgelegten Heimroutern und manchen Firewalls dürfen per UDP übertragene DNS-Pakete nicht größer als 1232 Bytes sein. Sind sie es doch, dann müssen sie fragmentiert werden, aber die veralteten Systeme verwerfen UDP-Fragmente aus vermeintlichen Sicherheitsgründen. Nun könnten DNS-Server ersatzweise auf das Transmission Control Protocol (TCP) umschalten, aber manche sind dafür nicht ausgelegt. Deshalb können übergroße DNS-Antworten versanden, sodass der Verbindungsaufbau scheitert.

Abhilfe ist in Sicht: Zwei Forscher haben kürzlich einen Mechanismus vorgeschlagen, mit dem ein Resolver übergroße DNS-Nachrichten stückweise vom DNS-Server abrufen kann (siehe ct.de/yzhd). Damit ließe sich die aus Empfängersicht unangekündigte Fragmentierung vermeiden. Doch bis eine solche Methode standardisiert wird, kann es Jahre dauern.

Deshalb kann man die Zwischenergebnisse von Wisiol und Kollegen zurzeit als gelbe Ampel für Falcon512 sehen: Sie fanden heraus, dass nur ein Teil der Falcon512-signierten DNS-Antworten unterhalb der wünschenswerten UDP-Grenze blieb und raten dazu, für DNSSEC weitere Alternativen zu suchen. Wisiol sieht die schon 2013 beschriebenen Algorithmen Bimodal Lattice Signature Schemes (BLISS) als gute Inspirationquelle. BLISS sei das erste kommerziell eingesetzte Quantencomputer-sichere Signaturverfahren. Doch in Analysen des NIST schneidet BLISS schlecht ab, weil die geprüften Varianten das geforderte Sicherheitsniveau 5 nicht erreichen. Dafür fordert das NIST unter anderem, dass Kandidaten mindestens so schwer zu knacken sind wie AES 256 (exhaustive key search). Da hilft es wenig, dass BLISS kleinere Signaturen erzeugt als Falcon.

Hash-Bäume als Notnagel

Burt Kaliski, Chief Technology Officer von VeriSign, schlägt in einem Blogpost Signaturen auf Basis von Merkle Trees vor. Geht es nach Kaliski, könnte man bei einem solchen Hash-Baum aus DNS-Einträgen kürzere Signaturen erhalten.

Unterdessen hat das NIST im Dezember 2022 auf seiner vierten Konferenz die nächste Runde zur Algorithmensuche eingeläutet. Vorschläge nimmt das Institut bis zum 1. Juni 2023 an. Hauptsächlich sei man an zusätzlichen Signaturmethoden für „allgemeine Zwecke“ interessiert. Aber spezielle Methoden „kommen auch in Frage, beispielsweise solche, die sehr kurze Signaturen erzeugen“. Das klingt nach einer weiteren Tür für neue DNSSEC-Algorithmen. Die genaue Standardisierung der ersten PQC-Methoden will das NIST jedenfalls erst 2024 in Angriff nehmen. *(dz@ct.de)* c't

DNS-Falcon GitHub-Projekt, PQC-Infos:
ct.de/yzhd