Analyse und Implementierung einer Multi-Faktor-Authentifizierung mit Shamir Secret Sharing

Nicolas Proske
Ostbayerische Technische Hochschule Amberg-Weiden
Moderne Anwendungen der Kryptographie
E-Mail: n.proske@oth-aw.de
Matr.-Nr.: 87672270

***Zusammenfassung*—Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Ut purus elit, vestibulum ut, placerat ac, adipiscing vitae, felis. Curabitur dictum gravida mauris. Nam arcu libero, nonummy eget, consectetuer id, vulputate a, magna. Donec vehicula augue eu neque. Pellentesque habitant morbi tristique senectus et netus et malesuada fames ac turpis egestas. Mauris ut leo. Cras viverra metus rhoncus sem. Nulla et lectus vestibulum urna fringilla ultrices. Phasellus eu tellus sit amet tortor gravida placerat. Integer sapien est, iaculis in, pretium quis, viverra ac, nunc. Praesent eget sem vel leo ultrices bibendum. Aenean faucibus. Morbi dolor nulla, malesuada eu, pulvinar at, mollis ac, nulla. Curabitur auctor semper nulla. Donec varius orci eget risus. Duis nibh mi, congue eu, accumsan eleifend, sagittis quis, diam. Duis eget orci sit amet orci dignissim rutrum.**

***Schlüsselwörter*—MFA, Secret Sharing**

I. Einleitung

In der heutigen digitalen Welt, in der eine überwältigende Menge an Daten generiert, gespeichert und über verschiedene Plattformen übertragen wird, ist der Bedarf an Datenschutz und Datensicherheit relevanter denn je. Die mit der Digitalisierung einhergehenden Möglichkeiten bergen ein erhebliches Risiko für Datendiebstahl, unbefugten Zugriff und Cyberangriffe. Obwohl laut einer Umfrage [1, S. 23] die Hälfte der Erwachsenen weltweit glauben, dass die von ihnen ergriffenen Maßnahmen ausreichen, um sich gegen Identitätsdiebstahl zu schützen, sind 63 Prozent darüber besorgt, dass ihre Identität gestohlen wird. Weiter fühlen sich knapp sieben von zehn Menschen heute anfälliger für Identitätsdiebstahl als noch vor ein paar Jahren. Ein wesentlicher Grund für die Zunahme von Identitätsdiebstahl liegt neben zu schwachen Passwörtern hauptsächlich daran, wie Menschen damit umgehen. Bei einer Frage bezüglich der mehrmaligen Verwendung derselben Benutzernamen und Passwörter haben 82 Prozent zugegeben, zumindest manchmal dieselben Anmeldedaten für unterschiedliche Konten zu verwenden. Knapp die Hälfte davon, etwa 45 Prozent, verwenden sogar immer oder in den meisten Fällen dieselben Zugangsdaten [2, S. 12].

A. Ein-Faktor-Authentifizierung

Lange Zeit haben Authentifizierungsmethoden auf einem einzelnen Identifikationsfaktor beruht, in der Regel einer Kombination aus Benutzername und Passwort. Wenn diese beiden Parameter über mehrere Dienste hinweg identisch sind, bedeutet dies, dass ein Angreifer, der ein einziges Konto kompromittiert, automatisch Zugriff auf die anderen Konten erhält — Dabei spielt die Stärke des Passworts keine Rolle. Dieser One-Factor-Authentication-Ansatz (OFA) hat jahrzehntelang das Rückgrat der Informationssicherheit gebildet. Dennoch hat sich angesichts der zunehmenden Komplexität von Cyberbedrohungen gezeigt, dass die Abhängigkeit von einem einzigen Faktor für die Authentifizierung eine Schwachstelle darstellt, die anfällig für verschiedene Verletzungen wie Brute-Force-Angriffe, Phishing und Keylogging ist. Diese Schwachstellen verdeutlichen, dass OFA für heutige Anwendungsfälle in aller Regel keine ausreichende Sicherheit mehr bietet.

B. Mehrfaktor-Authentifizierung

Multi-Factor-Authentication (MFA) stellt einen signifikanten Fortschritt in der Evolution der digitalen Sicherheitsmaßnahmen dar. Im Gegensatz zur Einzelfaktor-Authentifizierung, die üblicherweise auf einer einzigen Form des Nachweises wie einem Passwort basiert, erhöht MFA die Sicherheit durch zusätzliche Schutzebenen, indem mehrere unabhängige Zugangsdaten für die Authentifizierung erforderlich sind. Diese Zugangsdaten können in drei Hauptkategorien eingeteilt werden:

1) *Wissen*: Informationen, die der Benutzer kennt, wie Passwörter, PINs und Antworten auf geheime Fragen.
2) *Besitz*: Gegenstände oder Geräte, die der Benutzer besitzt, wie Smartphones, Chipkarten oder physische Schlüssel. Die Bestätigung des Besitzes kann verschiedene Formen annehmen, angefangen von der Entgegennahme und Eingabe eines per SMS an eine registrierte Telefonnummer gesendeten Codes bis hin zum Einsetzen eines physischen Schlüssels in ein Schloss.
3) *Eigenheit*: Biologische Merkmale, die einzigartig für den Benutzer sind, wie Fingerabdrücke, Netzhautmuster oder Gesichtserkennung.

Der Hauptvorteil von MFA gegenüber OFA liegt daher im schichtbasierten Ansatz. Selbst wenn ein Angreifer es schafft,

einen Authentifizierungsfaktor zu umgehen, bieten die verbleibenden Faktoren weiterhin Schutz. Eine Kompromittierung eines Faktors gefährdet also nicht die Gesamtsicherheit. Trotz der Stärken bringt eine MFA auch eigene Herausforderungen mit sich, wie beispielsweise die potenziell erhöhte Komplexität und die Notwendigkeit für Benutzer, mehrere Authentifizierungsfaktoren zu verwalten. Dennoch überwiegen die Vorteile der MFA oft diese potenziellen Nachteile, insbesondere in Umgebungen, in denen der Schutz sensibler Daten oberste Priorität hat.

C. Shamirs Secret Sharing

Shamirs Secret Sharing (SSS) ist ein kryptographischer Algorithmus, der am 1. November 1979 von Adi Shamir veröffentlicht wurde [3]. Es handelt sich um eine Methode, die die Aufteilung eines Geheimnisses in mehrere Teile, sogenannte Shares, ermöglicht. Jeder einzelne Share ist für sich genommen bedeutungslos und kann keinerlei Informationen über das ursprüngliche Geheimnis preisgeben. Wenn jedoch eine ausreichende Anzahl von Shares kombiniert wird, kann das Geheimnis rekonstruiert werden.

Shamirs Secret Sharing basiert auf dem Prinzip der Polynominterpolation in endlichen Körpern, wobei k Punkte ein Polynom vom Grad $k-1$ eindeutig definieren. Das (k, n)-Schwellenwertschema legt fest, wie viele k Shares benötigt werden, um das Geheimnis zu rekonstruieren, n ist größer k und bezieht sich auf die Gesamtzahl der Shares, in die das Geheimnis aufgeteilt wird.

Um dies anhand eines mathematischen Beispiels zu veranschaulichen, wird im Folgenden ein (2, 3)-Schwellenschema mit $k = 2$ und $n = 3$ betrachtet, bei dem das Geheimnis S der Zahl 42 entspricht. Sei $p = 43$ eine Primzahl mit $p > S$. Alle Berechnungen erfolgen im endlichen Körper $GF(p)$. Der erste Schritt besteht darin, ein Polynom vom Grad $k-1 = 2-1 = 1$ aufzustellen:

$$f(x) = mx + b \mod p$$

Die Konstante b entspricht dabei dem Geheimnis S. Aus Gründen der Übersichtlichkeit wird in diesem Beispiel $m = 4$ gewählt:

$$f(x) = 4x + 42 \mod 43$$

Im nächsten Schritt erfolgt die Berechnung von n Punkten in der Ebene. Dazu wird für $x = 1...n$ eingesetzt:

$$\text{Für } x = 1 : y_1 = f(1) = 4 * 1 + 42 \mod 43 = 3$$
$$\text{Für } x = 2 : y_2 = f(2) = 4 * 2 + 42 \mod 43 = 7$$
$$\text{Für } x = 3 : y_3 = f(3) = 4 * 3 + 42 \mod 43 = 11$$

Abbildung 1 zeigt alle berechneten Punkte $(1, 3), (2, 7), (3, 11)$, welche auf der durch das Polynom $f(x) = 4x + 42 \mod 43 = 4x - 1$ definierten Gerade liegen. Jeder Punkt (x_i, y_i) repräsentiert dabei einen Share.

Polynomdarstellung von $f(x) = 4x + 42 \mod 43$

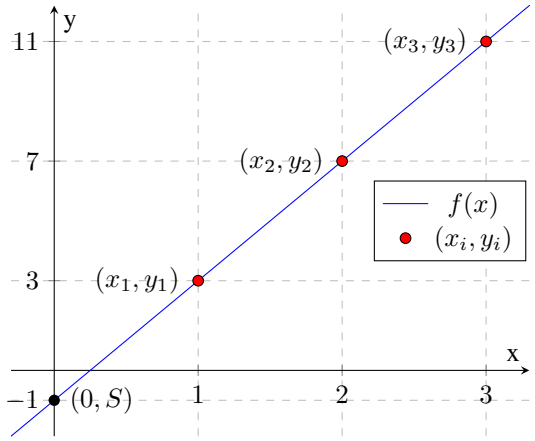

Abbildung 1. Polynomdarstellung für das Shamirs Secret Sharing Schema

LITERATUR

[1] Gen Digital Inc., „2023 Norton Cyber Safety Insights Report," Feb. 2023. Adresse: https://filecache.mediaroom.com/mr5mr_nortonlifelock/178041/2023%20NCSIR%20US-Global%20Report_FINAL.pdf (besucht am 05. 06. 2023).

[2] Morning Consult und IBM Security, „Security Side Effects of the Pandamic," Juli 2021. Adresse: https://filecache.mediaroom.com/mr5mr_nortonlifelock/178041/2023%20NCSIR%20US-Global%20Report_FINAL.pdf (besucht am 05. 06. 2023).

[3] A. Shamir, „How to share a secret," *Communications of the ACM*, Jg. 22, Nr. 11, S. 612–613, 1. Nov. 1979, ISSN: 0001-0782. DOI: 10.1145/359168.359176. Adresse: https://dl.acm.org/doi/10.1145/359168.359176 (besucht am 20. 06. 2023).