2. Managereigenschaften [Elektronische Ressourse]. – Das Regime des Zugriffes : https://karrierebibel.de/managereigenschaften/. – Das Datum des Zugriffes : 21.03.2022.

KONZEPTE DER KRYPTOGRAPHIE

КОНЦЕПЦИИ КРИПТОГРАФИИ

Сосукевич П.Н.
Научный руководитель: старший преподаватель Пужель Т.В.
Белорусский национальный технический университет

Kryptographie ist ein Muss für jeden modernen Entwickler, da sie uns überall umgibt. Alle unsere persönlichen Informationen, die über uns auf Remote-Computern gespeichert sind, alle unsere Passwörter erfordern grundlegende Kenntnisse der Kryptografie, um damit arbeiten zu können. Um damit zu arbeiten, barucht man aber die Mathematik und die Grundlagen des Universums nicht perfekt zu verstehen – eine einfache Kenntnis der Konzepte der Kryptographie ermöglicht, sie mit Leichtigkeit zu verwenden.

Weltweit wird die Kryptographie in zwei Arten unterteilt: Einweg- und Zweiweg-Verschlüsselung. Im ersten Fall werden die Daten in eine lange, vorzeichenlose Ganzzahl fester Länge umgewandelt, die als Hasch bezeichnet wird. Aufgrund der festen Länge ist der umgekehrte Vorgang mittels einer universellen Formel nicht möglich. Verschlüsselte Daten, einschließlich des Haschs, werden meistens in hexadezimaler Form dargestellt, dem sogenannten Digest, zum Beispiel a3fddc1de... Es gibt verschiedene Algorithmen, um einen Hasch zu erhalten, sogenannte Hasch-Funktionen, und das Erhalten eines Haschs wird als Hasching bezeichnet. Die heute am häufigsten verwendete Hasch-Funktion ist SHA256 (Standard-Hasch-Algorithmus). Das häufigste Beispiel für die Arbeit mit Hasching ist ein Passwort. Man hascht das Passwort und speichern den Hasch in der Datenbank. Wenn sich der Benutzer dann anmelden möchte, überprüft man den Hasch des eingegebenen Passworts mit dem in der Datenbank gespeicherten Hasch, und wenn sie übereinstimmen, ist der Benutzer kein Betrüger.

Es gibt doch mehrere Probleme. Erstens können verschiedene Passwörter denselben Hasch erzeugen. Diese Situation wird Kollision genannt. Aber dieses Problem wird in erster Linie durch die Qualität des Algorithmus und die Länge des Haschs gelöst. Moderne Hasches sind mehr als 256 Bit lang, und die Wahrscheinlichkeit einer Kollision ist extrem gering, weil Passwörter, die eine Kolli-

sion verursachen, haben in der Regel eine Länge, die größer ist als die vom Benutzer eingegebene.

Zweitens kümmern sich die meisten Benutzer nicht um ihre Sicherheit und geben Passwörter im Sinne von 123 oder standardmäßig platziert ein. Für die natürliche Komplikation von Passwörtern wird das sog. „Salz“ benutzt. „Salz“ wird zum ursprünglichen Passwort hinzugefügt und dann wie zuvor gehascht. „Salz“ wird in 2 Typen unterteilt: statisch und dynamisch. Das statische Salz ist konstant und wird in der Serverkonfiguration oder im Servercode selbst gespeichert. Es erfordert keinen zusätzlichen Speicherplatz, aber Passwörter werden vorhersehbarer, da nach dem Erlernen des statischen Salzes seine Vorteile aufgehoben werden und nur zusätzliche Zeit für das Hasching erforderlich ist. Daher wird in den meisten Fällen aus Sicherheitsgründen ein dynamisches Salz verwendet. Es wird in Abhängigkeit von den Daten des Benutzers (meistens auf seiner ID) oder zufällig generiert. Daher muss der Angreifer mit jedem Benutzer separat arbeiten. Ein Nachteil: muss im Fall der zufälligen Generierung das dynamische Salz zusammen mit dem Hasch gespeichert werden, was Gemeinkosten für Datenbankspeicher erzeugt.

Um die Integrität von Nachrichten anhand von Hasch zu überprüfen, wird der sog. HNAC (Haschbasierter Nachrichten-authentifizierungscode) verwendet. Er basiert sich darauf, dass die Eingabedaten gehascht werden und der Hasch auch an den Kunden gesendet wird, jedoch über einen anderen, sicheren Kanal. Wenn sich das Dokument während des Sendevorgangs nicht geändert hat, ist sein Hasch auf der Empfängerseite gleich. Wenn der Hasch über denselben Kanal wie das Dokument gesendet wird, kann ein Angreifer den Hash leicht fälschen, aber diese Methode eignet sich zum Schutz vor natürlichem Informationsverlust, beispielsweise durch eine schlechte Internetverbindung, und wird als Prüfsumme bezeichnet.

Im Fall der Zwei-Wege-Kryptographie werden die Daten in Blöcke fester Länge aufgeteilt und jeder von ihnen verschlüsselt. Die Entschlüsselung erfolgt in umgekehrter Reihenfolge: verschlüsselte Blöcke werden entschlüsselt und verkettet. Zur Verschlüsselung werden die sog. Schlüssel benutzt. Hier werden Verschlüsselungsmethoden in zwei Typen unterteilt: symmetrisch und asymmetrisch. Bei symmetrischen Verschlüsselungsverfahren wird ein Schlüssel verwendet, der beiden Parteien im Voraus bekannt ist. Bei asymmetrischen Verfahren werden zwei Schlüssel verwendet, das sogenannte Schlüsselpaar: öffentlicher und privater Schlüssel. Der öffentliche Schlüssel wird zur Verschlüsselung verwendet und kann frei weitergegeben werden. Der geschlossene wird zur Entschlüsselung verwendet und kann nicht offengelegt werden. Der Besitz eines öffentlichen Schlüssels gibt das Recht, eine Nachricht sicher an den Besitzer des entsprechenden privaten Schlüssels zu senden, aber keine Nachrichten von ihm zu empfangen, im Gegensatz zu symmetrischen Verfahren.

Der einfachste (und wahrscheinlich älteste) symmetrische Verschlüsselungsalgorithmus ist der sogenannte Cäsars Chiffre. Sein Wesen liegt in der Verschiebung der Buchstaben des Alphabets um eine bestimmte Verschiebung, d.h. A → B, B → C, C → D, ..., Z → A, um 1 nach rechts zu verschieben. Der Schlüssel hier ist „Shift 1 nach rechts“ und der Block ist jeder einzelne Buchstabe.

In der modernen Welt wird in der Regel ein Mixed-/Hybrid-Verschlüsselungsverfahren verwendet. Sein Wesen liegt darin, dass der Kunde sein eigenes Schlüsselpaar erstellt und den öffentlichen Schlüssel an den Server sendet. Da wird ein Sitzungsschlüssel für die spätere Kommunikation durch symmetrische Verschlüsselung erzeugt, mit dem vom Kunden erhaltenen öffentlichen verschlüsselt und zurückgegeben. Jetzt wird es möglich, durch symmetrische Verschlüsselung zu kommunizieren. Somit ist das Hauptproblem der symmetrischen Verschlüsselung gelöst: Der symmetrische Schlüssel muss irgendwie zwischen dem Kunden und dem Server geteilt werden, sowie das Hauptproblem der asymmetrischen Verschlüsselung: seine Langsamkeit. Der Sitzungsschlüssel macht nach dem Ende der Sitzung keinen Sinn mehr und wird einfach gelöscht.

Standardmäßig können asymmetrische Verschlüsselungsalgorithmen nur mit dem öffentlichen Schlüssel verschlüsselt und nur mit dem privaten Schlüssel entschlüsselt werden. Aber wenn der Algorithmus das Gegenteil kann – sich mit privaten Schlüsseln verschlüsseln und mit öffentlichen Schlüsseln entschlüsseln – dann eröffnen sich ihm neue Möglichkeiten, die sogenannten digitalen Signaturen. Sie sind wie Stempel: sie werden benötigt, um sicherzustellen, dass die Nachricht aus vertrauenswürdigen Händen kommt. Von der gesamten verschlüsselten Nachricht wird ein Hasch genommen, der wiederum mit einem privaten Schlüssel verschlüsselt wird und eine digitale Signatur bildet, und der öffentliche Schlüssel und dieselbe Signatur werden an den Empfänger übertragen. Durch die Entschlüsselung der Signatur erhält der Empfänger den Hasch des Dokuments. Auf Empfängerseite wird der entschlüsselten Nachricht ein Hasch entnommen und mit dem vom Absender empfangenen verglichen. Wenn sie gleich sind, hat der Absender die Nachricht verschlüsselt.

Diese Konzepte sind allgegenwärtig und sollten jedem modernen Programmierer bekannt sein, da sicheres Messaging und Hasching überall verwendet werden.

Das Ziel der Kryptographie besteht im Schutz von Nachrichten, Datenbeständen und sensiblen Informationen. Wer Informationen schützt, nimmt anderen die Möglichkeit, diese Informationen zum eigenen Vorteil nutzen zu können. Der Grundsatz der Vertraulichkeit bedeutet, dass nur berechtigte Personen verschlüsselte Informationen wieder entschlüsseln und lesen dürfen. Der Schutz von Daten ist wichtig, weil Informationen in den falschen Händen dazu führen können, dass sie missbraucht werden. Zusammengefassend kann man sagen,

dass die Kryptographie das Ziel hat, Informationen verschlüsselt, also für Dritte unverständlich, übermitteln zu können.

Bei der Anwendung der Kryptographie bestehen noch Probleme in mehrfacher Hinsicht: technische (z.B. fehlende Standards), juristische (z.B. inhomogene Rechtsgrundlage im Bereich des internationalen Privatrechts), gesellschaftspolitische (z.B. bzgl. Kontrollmöglichkeiten/-notwendigkeiten des Staates). Ferner sind Fortschritte bezüglich der Entschlüsselungsmöglichkeiten denkbar und sie müssen realisiert werden.

Литература

1. Kryptographie – Deffinition und Arten der Verschlüsselung [Elektronische Ressourse]. – Das Regime des Zugriffes : https://www.hornetsecurity.com/de/wissensdatenbank/kryptographie/?_adin=02021864894. – Das Datum des Zugriffes : 19.03.2022.

2. Kryptographie [Elektronische Ressourse]. – Das Regime des Zugriffes : https://www.enzyklopaedie-der-wirtschaftsinformatik.de/. – lexikon/technologien-methoden/Informatik--Grundlagen/Kryptographie Das Datum des Zugriffes : 19.03.2022.

3. Токарева, Н.Н. Симметричная криптография. Краткий курс: учебное пособие / Н.Н. Токарева. – Новосибирск, 2012. – 234 с.

4. Шнайдер, Брюс. Прикладная криптология. Протоколы, алгоритмы, исходные тексты на языке Си / Брюс Шнайдер. – М.: Изд-во ТРИУМФ, 2013. – 816 с.

INNOVATIVE VERPACKUNGEN DER ZUKUNFT

ИННОВАЦИОННАЯ УПАКОВКА БУДУЩЕГО

Грицель А.Н., Максимович А.В.
Научный руководитель: ст. преподаватель, Станкевич Н.П.
Белорусский национальный технический университет

Die Verpackungsmaterialien müssen heute immer mehr können: Sie müssen nicht nur die Waren vor Beschädigung und Verunreinigung schützen, sondern auch nachhaltig und ressourceneffizient hergestellt werden und recycelbar oder wiederverwendbar sein. Die Verpackungsindustrie in Hinblick auf nachhaltige und innovative Verpackungen macht heute große Fortschritte, um mit den traditionellen Kunststoffverpackungen zu konkurrieren. Einige dieser innovativen