Einmalpassw?rter (TANs) - Grundlagen, Anwendungen, Generierung

Jakob Lehner, Andreas Riedler

Communication Engineering, Institut f?r Wirtschaftsinformatik
Freist?dterstrasse 315, 4040 Linz, ?sterreich
http://www.ce.uni-linz.ac.at\\

Zusammenfassung In dieser Seminararbeit werden die Grundlagen und Anwendungen von TAN-Verfahren erl?utert und in einer Fallstudie gegen?bergestellt und verglichen.

Key words: TAN, Einmalpassw?rter, Two-Factor-Authentication

1 Einleitung

Bussiness Services; Was sind Business Services? Warum ist Business Services wichtig? Um die Sicherheit von Business Services speziell im Kontext des eCommerce zu erh?hen, setzen Banken, Regierungen und andere sicherheitssensitive Industrien Einmalpassw?rter ein. Bei einer Authentifikation mit Einmalpassw?rtern, besitzen die Benutzer mehrere Passw?rter, welche jedoch nur einmal verwendet werden. Welche Vorteile bringt das?
Ziel dieser Arbeit ist es Grundlagen, Konzepte zur Generierung und Anwendungen von Einmalpassw?rtern zu erl?utern. Zu Beginn werden die wesentlichen Grundlagen und anschlie?end die g?ngigsten Verfahren zur Generierung und Verteilung von Einmalpassw?rtern vor- und gegen?bergestellt. Zum Abschluss der Arbeit wird anhand eines konkreten Anwendungsgebietes der Einsatz von Einmalpassw?rtern aufgezeigt.

Bei den Verfahren noch r?ckbeziehen auf Grundlagen?

2 Grundlagen

In diesem Teil der Arbeit sollen die grundlegenden Konzepte zur Authentifizierung mit Einmalpassw?rtern erl?utert werden. Dazu werden zu Beginn die Arten der Authentifizierung vorgestellt und wie Einmalpassw?rter einzuordnen sind. Im Anschluss werden die verschiedenen Konzepte zur Generierung von Einmalpassw?rtern vorgestellt.

2.1 Arten der Authentifizierung

Die Unterscheidung von Authentifizierungsmechanismen erfolgt in der Regel in die drei Arten Wissen, Besitz und k?rperliche Merkmale. Bei einer Authentifizierung mittels Wissen hat der Benutzer sicherzustellen, dass er ?ber ein bestimmtes

Wissen verf?gt. Dies ist in der Regel ein Passwort, eine Personal Identification Number(PIN) oder ein kryptographische Geheimnisses. Von einer Authentifizierung durch Besitz spricht man, wenn der Benutzer den Besitz einer bestimmten Sache belegen kann. Dabei muss es sich nicht nur um physische Sache wie Chipkarten oder Tokens sondern auch Software, welche ein g?ltiges Passwort f?r die Authentifizierung erzeugt, ist eine solche Sache. Erfolgt die Authentifizierung ?ber k?rperliche Merkmale muss sich der Benutzer ?ber biometrische Mechanismen wie Fingerabdruckscan oder Stimmanalyse zu erkennen geben.[1] Jede dieser Arten zur Authentifizierung bietet unterschiedliche Vor- und Nachteile hinsichtlich Komplexit?t, Sicherheit und Benutzerfreundlichkeit. Auf diese Aspekte wird in dieser Arbeit jedoch nur hinsichtlich Einmalpassw?rtern und in einem der folgenden Kapitel eingegangen.

Wird nur eine der drei genannten Arten zur Authentifizierung verwendet, so spricht man von einer Single-Factor-Authentication. Dies ist der Fall wenn die Authentifizierung nur durch die Eingabe eines Passwortes erfolgt. Single-Factor-Authentication ist die schw?chste Form der Authentifizierung da ein Passwort ausspioniert, ein Token gestohlen oder ein Fingerabdruck nachgemacht werden kann. Werden hingegen zwei Arten der Authentifizierung miteinander kombiniert, nennt man dies eine Two-Factor-Authentication. Durch Hinzuf?gen eines zweiten Indetifiers wird die Sicherheit des Authentifizierungsprozesses erh?ht. Zum Beispiel kann eine Authentifizierung mittels Passwort und Token erfolgt. Somit muss der Benutzer zus?tzlich zu dem Wissen(Passwort) eine Sache(Token) besitzen. Von einer Three-Factor-Authentication spricht man wenn alle drei Arten zusammen eingesetzt werden. Typischerweise ist, zus?tzlich zu Passwort und Token, die biometrische Indetifikation der dritte Faktor bei einer Three-Factor-Authentication. Dies ist die st?rkste Form der Authentifizierung, da der Benutzer zus?tzlich zu Wissen(Passwort) und Sache(Token) auch die biometrischen Merkmale haben muss um eine Authentifizierung durchf?hren zu k?nnen.[2]

Einmalpassw?rter werden in der Regel zur Two-Factor-Authentication verwendet. Der Initiale Login erfolgt mit Kennwort und Passwort, welche den ersten Faktor darstellen. Als zweiter Faktor dient das Einmalkennwort, dass in einem zweiten Schritt eingegeben wird. Typische Anwendungsbereiche f?r Einmalpassw?rter sind Remote-Zug?nge zu Systemressourcen, Zug?nge zu internen Netzwerken von Organisationen und Anwendungen im e-Business wie zum Beispiel Online-Banking.[3] Auf die Anwendungen von Einmalpassw?rtern wird im Kapitel Anwendungen noch n?her eingegangen.

2.2 Konzepte zur Generierung von Einmalpassw?rtern

Nach dem wir nun die verschiedenen Arten der Authentifizierung erl?utert und Authentifizierung mittels Einmalpassw?rtern eingeordnet haben, werden wir in diesem Teil die wesentlichen Konzepte zur Generierung von Einmalpassw?rtern vorstellen. Zuerst werden wir eine Einf?hrung in Einweg-Hash-Funktionen geben, da diese f?r die Berechnung von Einmalpassw?rtern herangezogen werden. Anschlie?end leiten wir zu den Methoden zur Generierung von Einmalpassw?rtern ?ber.

Einweg-Hashfunktionen Sind Hashfunktionen, die nur in eine Richtung funktionieren. Dies bedeutet, dass sich zu einer Eingabe ein Hashwert problemlos berechnen l?sst. Jedoch ist es schwer ausgehend von einem bestimmten Hashwert, denn Originalwert zu berechnen. Schwer bedeutet dabei, dass es vom Rechenaufwand her ist, aus einem Hashwert das Original zu berechnen.[4]

Hashfunktionen legen einen endlichen Bildbereich, der auch als Adressbereich bezeichnet wird, fest. Dieser Adressbereich ist meist erheblich kleiner als der Urbildbereich, der auch das Universum genannt wird. Hashfunktionen bilden jedes Objekt eines Universums auf eine Hashadresse ab. Da der Bildbereich meist erheblich kleiner ist als das abzubildende Universum, k?nnen Kollisionen auftreten.[5]

Die Sicherheit einer Einweg-Hashfunktion liegt in ihrer Einweg-Eigenschaft, da die Hashfunktion ?ffentlich und somit das Verfahren nicht geheim ist. Die Ausgabe steht in keinem nachvollziehbaren Zusammenhang mit der Eingabe und durch die ?nderung eines Bits in der Eingabe ?ndert sich im Mittel die H?lfte aller Bits im Hashwert. Eine gute Einweg-Hashfunktion ist au?erdem kollisionsresistent. Dies bedeutet das es erstens praktisch unm?glich ist zwei Originalwerte mit demeselben Hashwert zu erzeugen und zweitens soll es nicht m?glich sein, zu einem gegebenen Hashwert eine Nachricht zu finden, die den selben Hashwert liefert.[4]

The S/Key One-Time Password System Das S/Key One-Time Password System basiert auf den Ideen von Leslie Lamport. Leslie Lamport adressiert mit seinem Verfahren zwei wesentliche Sicherheitsrisiken der Authentifizierung mit Passw?rtern. Zum ersten nennt er das Risiko, dass ein Angreifer Zugang zur Passwortdatei erlangt. Das zweite Sicherheitsrisiko, auf das sich Lamport bezieht, ist die Gefahr die beim Austausch und ?berpr?fen des Passworts entsteht. Ein Angreifer k?nnte dabei an das Passwort gelangen.[6]

Das erste Problem l?st Lamport durch die verschl?sselte Ablage des Passwortes auf dem Zielrechner. Die Verschl?sselung erfolgt mittels Einwegfunktion. Durch den Einsatz einer Sequenz von Passw?rtern l?st Lampert das zweite Problem. Diese Sequenz von Passw?rtern kann zum einen Initial gew?hlt werden oder der Benutzer sendet beim aktuellen Login das verschl?sselte Passwort f?r den n?chsten Login. Beide Varianten weisen jedoch M?ngel auf. Bei der ersten m?ssten sowohl Benutzer als auch das System eine umfangreiche Passwortliste speichern und verwalten. Die Schw?che der zweiten Variante liegt in der Kommunikation zwischen Benutzer und System. Durch Kommunikationsfehler oder durch Angreifer ist es m?glich, dass das System denn verschl?sselten Wert des Passwortes f?r die n?chste Anmeldung nicht oder falsch erh?lt.[6]

Lampert l?st die angef?hrten Probleme durch eine wiederholte Ausf?hrung einer Einwegfunktion F auf ein Passwort x. Dies bedeutet, dass das Ergebnis von $F(x)$ als Input f?r das n?chste Passwort verwendet wird. Eine Sequenz von Passw?rtern f?r den Benutzer ist somit

$$F^{n-1}(x), ..., F(F(F(F(x))), F(F(x))), F(x), x$$

und die Passwortsequenz y auf dem System lautet

$$F^n(x), ..., F(F(F(F(x))), F(F(x))), F(x).$$

Dies bedeutet das jedes Benutzerpasswort, jenes Passwort ist, mit dem das System das n?chste Passwort bestimmen kann. Das System muss mit dem Wert $y_1 = F^n(x)$ initialisiert werden. Nun muss es sich nur mehr das letzte Passwort merken welches vom Benutzer gesendet wurde.[6]

Das S/Key One-Time Password System(SKOTP) ?bernimmt die Ideen von Lamport und wurde erstmals auf einem Unix System implementiert. Die Ziele dieses Systems sind der Schutz gegen **Eavesdropping**, einfache Benutzbarkeit, automatische Ausf?hrung, keine Verwendung von geheimen Algorythmen und keine Speicherung von Geheimnissen. Wie bei Lamport soll das SKOTP Schutz gegen passives **Eavesdropping** bieten, im dem keine Information zwischen System und Benutzer wechselt, die zur Authentifikation verwendet werden kann. Die einfache Ausf?hrbarkeit soll die Benutzerakzeptanz erh?hen und die automatische Ausf?hrung soll eine leichte Konvertierung auf ein tokenbasiertes System erm?glichen. Also ein Wechsel von Authentifizierung durch Wissen auf Authentifizierung durch Besitz einer Sache. Dadurch das keine geheimen Algorythmen verwendet werden, kann das SKOTP von der Industrie evaluiert werden. Sicherheitsl?cken k?nnen so mit gr??erer Warscheinlichkeit entdeckt. In Bezugnahme auf Lamport erfolgt beim SKOTP ebenfalls keine Speicherung von geheimen Schl?sseln oder Passw?rtern auf dem Host. Dies vermindert die Attraktivit?t des Hosts als Ziel.[7] Als Basis f?r das Verfahren dient ein geheimes Passwort s, welches zwischen Benutzer und seinem Arbeitsplatzrechner vereinbart wurde. Hervorzuheben ist hierbei noch einmal, dass dem Server das Geheimnis s nicht bekannt sein muss. Also muss weder ein Austausch des Geheimnisses erfolgen noch muss der Server das Geheimnis verwalten. Die Ausf?hrung erfolgt in den zwei Schritten Vorbereitung Authentifizierung.[5] Im Vorbereitungsschritt wird

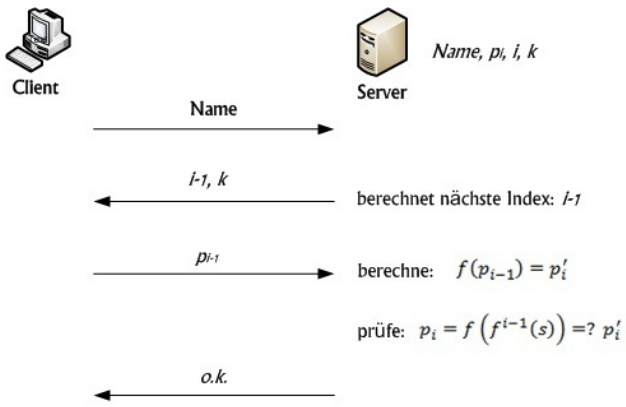

Abbildung 1. Schematische Darstelleung des S/Key Schemas[5]

vom Server zum Client ein Seed k in Klartext gesendet. Dieser Seed ist eindeutig f?r den Benutzer auf dem entsprechenden Server und dient dazu, dass ein Benutzer das gleiche Passwort auf mehreren Rechnern verwenden kann. Aus dem Geheimnisses s und dem Seed-Wert k berechnet der Client die Folge der benutzbaren Passw?rter $p_1, ..., p_n$ wie folgt[5]:

$$p_i = f^i(s|k) \text{ f?r } i = 1, ..., n$$

F?r die Authentifizierung des Clients zum Server werden ausschlie?lich diese Einmalpassw?rter p_i verwendet. So erfolgt nie ein Austausch des Geheimnisses s. F?r den Benutzer ?ndert sich nichts gegen?ber eine herk?mmlichen Anmeldung. Er weist sich gegen?ber dem Client mit seinem Geheimnis s als authentisches Subjekt aus.[5] Nach der i-ten erfolgreichen Authentifizierung gilt, dass der Server das Passwort p_i ?berpr?ft und zusammen mit dem Index i protokolliert hat. Erfolgt eine neuerlicher Login-Anfrage durch den Client-Rechner, wird er vom Server aufgefordert, das $(i-1)$-te Passwort vorzuweisen. F?r diesen Zweck sendet der Server die laufende Nummer $i-1$ sowie den Seed-Wert k an den Client-Rechner. Daraus berechnet(oder w?hlt es aus einer Liste aus) und ?bertr?gt der das entsprechende Passwort $p_i - 1$ zum Server. Das Passwort $p_i - 1$ erh?lt man durch wiederholtes($i - 1$ mal) Anwenden der Funktion f auf das Geheimnis s welches mit dem Seed k angereichert wurde. Ob das Passwort $p_i - 1$ korrekt ist, kann der Server durch die einmalige Anwendung der Funktion f auf $p_i - 1$?berpr?fen. F?r das Passwort gilt[5]:

$$p_i = f^i(s|k) = f(f^{(i-1)}(s|k)) = f(p_{i-1})$$

Somit ist zu ?berpr?fen, ob gilt

$$f(p_{i-1}) = p_i$$

Bei einer ?bereinstimmung ist die Authentifizierung erfolgreich. Der Server ersetzt nun den Wert p_i durch das verbrauchte Passwort p_{i-1} und erniedrigt seinen Sequenzz?hler um eins.[5]

Die Sicherheit dieses Verfahrens ist abh?ngig von der Einwegeigenschaft der Funktion f und von der Qualit?t des zugrundeliegenden Geheimnisses s. Die ?bertragung des Passwortes p_i zwischen Client und Server erfolgt unverschl?sselt. Dadurch ist es einem Angreifer m?glich dieses zu beobachten. Jedoch ist es ihm nicht m?glich durch Kenntnis des Passworts p_i, das n?chste Passwort zu bestimmen. Da er das Geheimnis s nicht kennt, m?sste er das Urbild des Passworts $p - i$ wie folgt berechnen[5]:

$$p_{i-1} = f^{-1}(p_i)$$

Somit wird eine erfolgreiche Maskierung erschwert, jedoch nicht vollst?ndig ausgeschlossen. Ist es dem Angreifer m?glich das Passwort p_i welches vom Client zum Server gesendet wird, so abzufangen dass es den Server nicht erreicht, bricht dieser die Authentifizierung ab, ohne seinen Passwortz?hler zu vermindern. Der

Angreifer kann sich nun beim Server anmelden in dem er das Abgefangene Passwort p_i verwendet. Diese Schwachstelle kann jedoch beseitigt werden im dem der Server bei einem Fehlgeschlagenen Login den Passwortz?hler trotzdem vermindert.[5] Neben einer clientseitigen Maskierung ist auch eine Serverseitige m?glich. Maskiert sich ein Angreifer als Server und ?bermittelt dem Client eine Sequenznummer j, die wesentlich kleiner ist als die zuletzt Verwendete, so wird der Client dem Server das korrekte Passwort p_i ?bermitteln. Somit ist es dem Angreifer m?glich alle Sequenznummern $r \in j, ..., i-1$ des Original-Servers mit einem korrekten Passwort zu beantworten, indem er ausgehend vom erschlichenen Passwort p_j den Wert

$$f^{r-j}(p_j) = p_r$$

berechnet.[5]

Durch das Abfangen von Einmalpassw?rtern, der Sequenznummer i und dem Seed k entntsteht eine weiteres Sicherheitsproblem. Ein Angreifer kann mit diesen Werten einen W?rterbuchangriffe auf das geheime Passwort s durchzuf?hren. Bei einem W?rterbuchangriff muss der Angreifer mit allen m?glichen W?rtern s' eine S/Key-Berechnung durchf?hren. Das hei?t er muss die bekannte Hashfuntkion i-mal auf s', angereichert mit dem Seed k andwenden. Diese Problem kann dadurch gel?st werden, dass dem Benutzer durch das System ein geheimes Passwort s zugewiesen wird, welches eine gute Zufallszahl darstellt.[5]

Challange Response Mitchel: Comments on the SKEY user authentication scheme

Zeitbasierend Claudia Eckert: IT Sicherheit OTP-Tokens/RSA SecurID

3 Generierung und Verteilung

3.1 TAN - Liste

TAN Liste, iTAN

3.2 SMS

3.3 Mobiltelefon

3.4 Tokens

3.5 Einordnung und Vergleich der Technologie

Welche Art der Generierung wird verwendet? Sicherheit? Vorteile und Nachteile?

4 Anwendung

Spezielle Case Studies, zwei oder mehr Beispiele, die Aufgrund einer Skala z.B. Sicherheit, Aufwendigkeit usw.bewertet werden.

alte Quellen:

Gianluigi Me et al: A mobile based approach to strong authentication on Web
Kuan-Chieh Liao: A One-Time Password Scheme with QR-Code Based on Mobile Phone
Fadi Aloul: Two Factor Authentication Using Mobile Phones
Telvis E. Calhoun Jr.: Authentication in 802.11 LANs using a Covert Side Channel
Binod Vaidya: Authentication Mechanism Using One-Time Password for 802.11 Wireless LAN
Chun-Ming Leung: Depress Phishing by CAPTCHA with OTP
Daiki NObayashi: Development of Single Sign-On System with Hardware Token and Key Management Server
Paras Babu Tiwari: Single Sign-on with One Time Password
Wen-Chung Kaol: Integrating Flexible Electrophoretic Display And One-Time Password Generator in Smart Cards
Yongjin Lee: One-Time Templates for Face Authentication
Christian Gilmore: Secure Remote Access to an Internal Web Server
Liang Fang: Secure Password-Based Authenticated Key Exchange for Web Services

neue Quellen:

MohammedAlZomai: An Experimental Investigation of the Usability of Transaction Authorization
Roberto Di Pietro: A Two-Factor Mobile Authentication Scheme
Christos K. Dimitriadis: Analyzing the Security of Internet Banking
Anders Moen Hagalisletto:Analyzing two-factor authentication devices
Cornel de Jong: Online authentication methods

5 Fazit

6 Quellen

[1]Two-factor authentication Siemens [2]Mike Meyers' CompTIA Security+ Certification Passport, Second Edition Von T. J. Samuelle [3]Information security architecture: an integrated approach to security in the ... Von Jan Killmeyer Tudor [4]Angewandte Kryptographie Bruce Schneider [5]IT-Sicherheit Claudia Eckert [6]Password Authentication with Insecure Communication; Leslie Lamport [7]The S/Key One-Time Password System; Neil M. Haller