Stefanie Langer

Sicherheit von passwortbasierten Authentifizierungssystemen

Bachelorarbeit

Diplom.de

Bibliografische Information der Deutschen Nationalbibliothek:

Bibliografische Information der Deutschen Nationalbibliothek: Die Deutsche Bibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de/ abrufbar.

ISBN: 9783961160181

Stefanie Langer

Sicherheit von passwortbasierten Authentifizierungs-systemen

Diplom.de

Stefanie Langer

Thema der Arbeit
Sicherheit von passwortbasierten Authentifizierungssystemen

Stichworte
IT-Sicherheit, Passwortsicherheit, Single Sign-On (SSO), Authentifikation, Kerberos

Kurzzusammenfassung
Diese Arbeit hat die Untersuchung zweier Thesen zum Ziel. Es soll beleuchtet werden, ob regelmäßige/erzwungene Passwortwechsel zum einen und die Verwendung von Single Sign-On-Systemen zum anderen die Sicherheit erhöhen. Es werden zunächst Grundlagen zur Begrifflichkeit von Sicherheit sowie psychologische Grundlagen erläutert. Nachfolgend werden Konstruktion, Verwendung und Sicherheitsrisiken von Passworten erläutert, um anschliessend die erste These zu untersuchen. Im Anschluss werden passwortbasierte Authentifikationssysteme am Beispiel von Single-Sign On und unter der Verwendung von Kerberos definiert, beschrieben und deren Sicherheitsrisiken erläutert, um die zweite These zu prüfen.

Stefanie Langer

Title of the paper
Security of password-based authentification systems

Keywords
IT-security, password security, single sign-on (SSO), authentification, Kerberos

Abstract
This document targets on the investigation of two theses. It should be shown if periodical/forced password change on one hand, and the use of single sign-on systems on the other hand increases security. At first, the basics concepts of security and psychological basics were explained. Subsequently, construction, use and safety risks of passwords are explained in order to examine the first thesis. Afterwards, password-based authentication systems using the example of single sign-on and Kerberos are defined, described and their security risks were explained, followed by the examination of the second thesis.

Inhaltsverzeichnis

1. Einleitung

Heutzutage dominiert die elektronische Datenverarbeitung die Mehrheit der Arbeitsplätze. Daten, die noch vor einigen Jahrzehnten ganze Räume mit Aktenschränken füllten werden nun digital vorgehalten. Mit dieser Menge an Daten geht eine große Verantwortung einher - um den Zugriff zu regulieren und die Daten vor unberechtigtem Zugriff zu schützen findet nahezu an jedem beruflich genutzten Computer eine Authentifizierung des Benutzers mit einem Passwort statt. In einer Welt, in der das Internet auf mobilen und stationären Geräten allgegenwärtig ist, beschränkt sich die Nutzung von passwortbasierten Authentifikationssystemen nicht mehr nur auf den beruflichen Gebrauch. Soziale Netzwerke, Online-Banking, die Nutzung von Foren, E-Commerce-[1] oder auch E-Learning Plattformen erfordern stets eine Registrierung mit Benutzernamen und Passwort.

Die Sicherheit der Daten hängt bei einer passwortbasierten Authentifikation maßgeblich von der Qualität des Passworts ab. Hier trifft der Anwender die Entscheidung wie es lauten soll, abhängig von einer eventuellen Vorbildung oder Vorschrift durch das authentifizierende System. Gerade im beruflichen Umfeld hat der Benutzer Zugriff auf verschiedenste, individuell geschützte Anwendungen und Programme. Meist handelt es sich um eine Windows-Umgebung, die nach dem Einloggen weitere Programme zur individuellen Nutzung zur Verfügung stellt. Hier hat sich inzwischen die Nutzung von sogenannten Single Sign-On-Verfahren durchgesetzt die dem Benutzer erlauben, bereits nach einer initialen Authentifizierung Zugriff auf alle zu Verfügung gestellten Programme zu haben.

1.1. Motivation und Ziel

Obwohl passwortbasierte Authentifizierungen allgegenwärtig sind scheint dem durchschnittlichen Nutzer das damit verbundene Risiko, wichtige Daten durch mangelhaften Schutz offenzulegen, nicht bewusst zu sein.

Im Gegenzug zur Standard-Authentifizierung, bei der für jede Benutzung eines Systems oder Programms die Eingabe von Benutzernamen und Passwort notwendig ist sollen Single

[1] z.B. Online-Versandhäuser wie Amazon.de, Zalando.de oder Otto.de

Sign-On-Systeme die Arbeit erleichtern, indem der Workflow nicht durch wiederkehrende Authentifizierungen und den dadurch zu merkenden, verschiedenen Passworten unterbrochen wird. Doch gilt es zu klären, ob durch diese Erleichterung auch noch die notwendige Sicherheit gewährleistet werden kann - gerade dann, wenn der Anwender sein Passwort mangelhaft auswählt.

Diese Arbeit ist in zwei Schwerpunkte unterteilt: zunächst werde ich prüfen, welche Maßnahmen zur Verbesserung der Passwortsicherheit bereits existieren und deren Sinnhaftigkeit bewerten. Hierbei soll auch der psychologische Hintergrund des Benutzers betrachtet werden um zu ergründen, warum Menschen sich auf eine bestimmte Art und Weise verhalten und hierdurch zum vielbeschriebenen „Risikofaktor Mensch“ werden. Im Anschluss an die Untersuchung der Passwortsicherheit soll folgende These überprüft werden:

> Erhöhen vorgeschriebene Passwortwechsel innerhalb fester Zeiträume (z.B. monatlich, dreimonatlich) die Passwortsicherheit?

Den zweiten Schwerpunkt bildet die Untersuchung von passwortbasierten Authentifikationssystemen. Besonderes Augenmerk liegt hier auf Authentifikationssystemen, die nach dem Single Sign-On Verfahren operieren. Diese werden kategorisiert und hinsichtlich ihrer Sicherheit untersucht, um im Anschluss die zweite Kernthese zu untersuchen:

> Erhöhen Single Sign-On-Systeme die Sicherheit?

Abschließend wird der Zusammenhang beider Thesen hergestellt und überprüft, ob die Verifizierung respektive Falsifizierung der Thesen auch in einem gemeinsamen Kontext gilt: Inwieweit ist die Sicherheit von Single Sign-On-Systeme davon abhängig, ob ein Passwort in regelmäßigen Abständen zu verändern ist?

1.2. Gliederung der Arbeit

Diese Arbeit gliedert sich in 6 Kapitel auf. Kapitel 2 klärt zunächst die grundlegenden Begrifflichkeiten Sicherheit und IT-Sicherheit, wonach Kapitel 3 einen Einblick in die psychologischen Grundlagen liefert und die menschliche Handlungsweise beleuchten soll.

Im Anschluss wird in Kapitel 4 der Begriff des Passwortes sowie der verschiedenen Arten von Passworten definiert sowie erläutert, welche Sicherheitsrisiken durch menschliche Einflussnahme bestehen. Verschiedene Gegenmaßnahmen und die Untersuchung der ersten Kernthese schließen das Kapitel ab.

Nach einer Erläuterung von passwortbasierten Authentifikationssystemen im Allgemeinen und Single Sign-On-Systemen sowie deren Technologie am Beispiel von Kerberos wird die zweite Kernthese untersucht.

Den Abschluss bildet der Schluss (Kapitel 6), der eine Zusammenfassung der Arbeit geben soll. Es folgt das Fazit dieser Arbeit sowie ein Ausblick auf aktuelle und zukünftige Entwicklungen.

2. Grundlagen

Sicherheit ist ein kontextsensitiver Begriff und hat nicht nur für jeden Menschen, sondern auch in Bezug auf z.B. die Informationstechnologie (IT)[1] unterschiedliche Ausprägungen und Bedeutungen. Dieses Kapitel will Begriffe abgrenzen und definieren sowie einen Überblick über diejenigen verschaffenen, die für diese Arbeit von grundlegener Relevanz sind.

2.1. Definition Sicherheit im Allgemeinen

Sicherheit bezeichnet einen Zustand des Sicherseins, Geschütztseins vor Gefahr oder Schaden bzw. das höchstmögliche Freisein von Gefährdungen[2]. Auf der Suche nach einer Definition kommen jedoch einige Aspekte zum Tragen, die eine Unterscheidung des Sicherheitsbegriffes erfordern. [Bun02] nimmt in seinem Artikel z. B. eine Unterteilung in vier Kategorien vor:

- Sicherheit bedeutet Gewissheit, Verlässlichkeit, Vermeiden von Risiken, aber auch Abwesenheit von bzw. Schutz vor Gefahren werden mit diesem Begriff assoziiert.
- Sicherheit meint aber auch Statussicherheit, Gewährleistung des erreichten Lebensniveaus und der Lebensumstände einzelner Menschen und/oder sozialer Gruppen sowie Bewahrung der gesellschaftlichen und politischen Verhältnisse, in denen Menschen leben und sich eingereichtet haben.
- Mit dem Begriff ist weiterhin ein bestimmtes institutionelles Arrangement assoziiert, das als geeignet erscheint, innere und äußere Bedrohungen einer sozialen und politischen Ordnung abzuwehren.
- Und schließlich wird Sicherheit im juristischen Sinne als Unversehrtheit von Rechtsgütern verstanden, die zu schützen und bei Verletzung wieder herzustellen Aufgabe der Rechtsordnung und des Staates ist.

Sicherheit kann auch die 100-prozentige Wahrscheinlichkeit des Zutreffens einer Aussage oder des (Nicht-)Eintreffens eines Ereignisses beschreiben (nach [BSHL12]).

[1] ebenso üblich ist die Bezeichnung Informations- und Kommunikationstechnologie (IKT).
[2] `http://www.duden.de/rechtschreibung/Sicherheit#Bedeutung1`

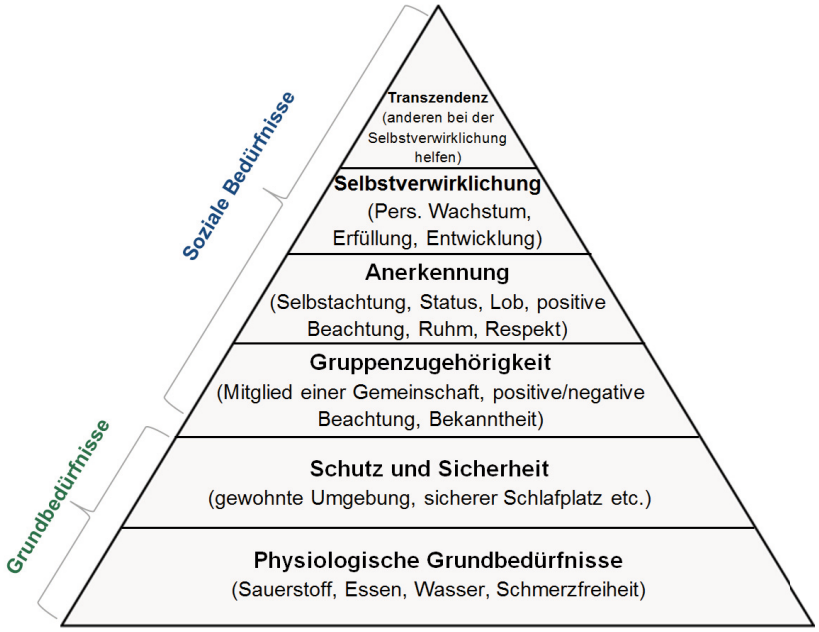

Abbildung 2.1.: Die Maslowsche Bedürfnispyramide frei nach A. H. Maslow

Abraham H. Maslow als wichtiger Vertreter der humanistischen Psychologie hat die grundlegenden menschlichen Bedürfnisse in seiner Pyramidendarstellung (siehe Abbildung 2.1 und vgl. [Ehl08]) hierarchisch angeordnet. Direkt nach den wichtigsten, den physiologischen Bedürfnissen wie Essen, Trinken, Schlaf und Schmerzfreiheit ordnet er das Bedürfnis nach Schutz und Sicherheit ein. Der Mensch strebt somit nach der Befriedigung seiner physiologischen Grundbedürfnisse nach Schutz und Sicherheit.

[GK08] unterscheidet zwischen den Risikobereichen Sicherheit und Gefahr, die durch das Grenzrisiko voneinander getrennt sind. Diese werden zwar als Gegensätze empfunden, gehören aber zum selben Maßstab: beides ist ein Schadensrisiko, das vom Grenzrisiko gleichermaßen verbunden und getrennt wird. Weder Gesetzgeber noch Technik können jedoch den Ort des Grenzrisikos effektiv festlegen, da dieser für jeden Einzelfall separat betrachtet und festgelegt werden muss. Auf diese Weise sind Sicherheit und Risiko untrennbar miteinander verbunden - die Erhöhung der Sicherheit kann nur durch Verringerung des Schadenrisikos erfolgen, wobei es keinen Zustand gibt, an dem kein Risiko besteht.

Sicherheit als Grundbedürfnis des Menschen kann es nur dann geben, wenn das Einzelfallabhängige Risiko als gering eingeschätzt wird. Sowohl gesetzliche Vorgaben als auch der Erfahrungsschatz eines Einzelnen hat maßgeblichen Einfluss auf das Empfinden einer Person.

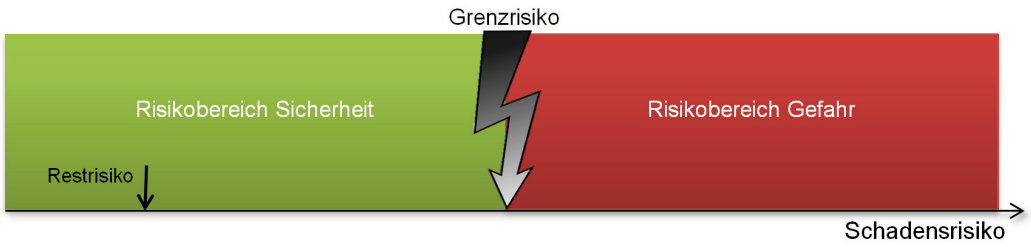

Abbildung 2.2.: Das Schadensrisiko als Maßstab von Sicherheits- und Gefahrenbereich, frei nach [GK08]

Wichtig zu berücksichtigen ist, dass sich die Risikoabschätzung und Sicherheitsempfindung durch verschiedenste Faktoren beeinflussen lässt (siehe auch: Unterkapitel 4.3.1, Social Engineering). Auch wenn ein Mensch bereits über ein eventuell eintretendes Risiko informiert ist findet die Sicherheitseinstufung individuell, und auch unter Berücksichtigung von Heuristiken (siehe auch: Kapitel 3.4, Heuristiken) statt.

Im Kontext dieser Arbeit soll daher von folgender, eigener Definition von Sicherheit ausgegangen werden:

Satz 2.1.1

Der Mensch empfindet Sicherheit genau dann, wenn er sich keines bestehenden Risikos bewusst ist.

2.2. Definition Sicherheit in der Informationstechnologie

> „IT-Sicherheit hat die Aufgabe, Unternehmen und deren Werte (Know-How, Kundendaten, Personaldaten) zu schützen und wirtschaftliche Schäden [...] zu verhindern.“ Claudia Eckert [Eck12, S. 1]

Die Begriffe IT-Sicherheit und Informationssicherheit werden in der Literatur häufig synonym verwendet, obwohl diese bei genauer Betrachtung unterschiedliche Ziele verfolgen. [Eck12] gibt erstmals einen Gesamtüberblick über die Materie, indem sie den Begriff Sicherheit als Maßstab vorgibt und diesen in vier Bereiche unterteilt (siehe auch Abbildung 2.3):

- **Funktionssicherheit** (engl. safety): Die Übereinstimmung der realisierten Ist-Funktionalität der Komponenten eines Systems mit deren Soll-Funktionalität ohne funktional unzulässige Zustände.
- **Informationssicherheit** (engl. security): die Eigenschaft eines funktionssicheren Systems unautorisierte Informationsveränderung oder -gewinnung zu vermeiden.
- **Datensicherheit** (engl. protection): Die Eigenschaft eines funktionssicheren und informationssicheren Systems, unautorisierte Zugriffe auf Systemressourcen und Daten als auch Informationsverlust (z.B. durch fehlende Backups) zu verhindern.
- **Datenschutz** (engl. privacy): die Fähigkeit einer natürlichen Person, die Erhebung und Verwendung und Weitergabe von deren personenbezogenen Daten zu kontrollieren (siehe auch [Bun13b]).

IT-Sicherheit bezeichnet somit weniger die Sicherheit als vielmehr den Schutz von Informationen, die elektronisch als Daten gespeichert und mithilfe von Informationstechnologie (IT) verarbeitet wurden, vor Bedrohungen : dem Nutzer selbst, Malware, Hacker oder Kriminellen (vgl. [Bru06]).

Abbildung 2.3 listet sowohl englisches als auch deutsches Sicherheitsvokabular auf, um eine bessere Übersicht zu gewähren.

Englisch	Deutsch	Oberbegriff
Safety	Funktionssicherheit, Betriebssicherheit	Begriff Sicherheit
Security	Informationssicherheit	
Protection	Datensicherheit, Datensicherung	
Privacy	Datenschutz	
Authenticity	Echtheit, Glaubwürdigkeit	Sicherheitsziele
Integrity	Manipulationssicherheit	
Confidentiality	Vertraulichkeit	
Availability	Verfügbarkeit	
Non Repudiation	Verbindlichkeit, Nicht-Abstreitbarkeit	

Abbildung 2.3.: deutsches und englisches Sicherheitsvokabular nach [Kli10]