

Benutzbare Benutzerauthentifizierung Security and Usability of Passwords

Technologien der Informationsgesellschaft

Sommersemester 2006

Matthias Bernauer

Institut für Informatik und Gesellschaft - Telematik

Übersicht

Grundlagen

Wozu Passwörter?

Was ist mit alternativen Authentifizierungsmethoden?

Was ist ein sicheres Passwort?

Usability

Was versteht man unter Benutzbarkeit?

Trade-off zwischen Sicherheit und Benutzbarkeit?

Ansätze zur Gestaltung sicherer und anwendungsfreundlicher Passworte

Authentifizierung

- **Wissen**

Passwörter, PINs, Question-Response-Verfahren, ...

[-] variierende Qualität, unbefugte Weitergabe, Sharing, schwer zu merken

[+] einfacher, billiger & korrekter Mechanismus, nahezu überall einsetzbar

- **Besitz**

RFID, Magnetkarten, Zertifikate, ...

[-] Verlust, Diebstahl, Weitergabe, Defekte, anfallende Kosten, Extrageräte

[+] verbesserte Sicherheit (Qualität), beschränkte Weitergabemöglichkeit

- **Sein**

Sprache, Iris, Fingerabdruck, Gesichtserkennung, u.v.a.

[-] Extrageräte, Merkmale veränderlich, sensorbedingte Erkennungsfehler

- **Kontext**

IP, Büro-Zugang, SID, Aufruf durch Parent-Prozedur, ...

Authentifizierung

- **Wissen**

Passwörter, PINs, Question-Response-Verfahren, ...

[-] variierende Qualität, unbefugte Weitergabe, Sharing, schwer zu merken

[+] einfacher, billiger & korrekter Mechanismus, nahezu überall einsetzbar

>> Passwörter gebräuchlichster Authentifizierungsmechanismus

>> häufiger Einsatz

Sicherheit

Unsichere Passwörter

- zu kleiner Zeichensatz
- zu kurze Passwörter
- kontext- oder nutzerbezogener Inhalt
- Wörterbucheinträge, Vornamen, Namen, Vereine, Markennamen
- Redundanzen
- bekannte Abkürzungen, Jahreszahlen, Geburtstage, Tel.Nr, KFZ-Zeichen
- Tastatur- und Eingabemuster
- Variationen bereits bestehender Passwörter
- 'test', 'passwort', 'kennwort', '123456', 'hallo'

Sicherheit

<i>Passwortlänge</i>	<i>Zahl der möglichen Passwörter</i>	<i>Zeitbedarf zum Knacken</i>
1	62	keiner
2	3844	keiner
3	238.328	keiner
4	14.776.336	1,4 Sekunden
5	916.132.832	1,5 Minuten
6	56.800.235.584	1,5 Stunden
7	3.521.614.606.208	4 Tage
8	218.340.105.584.896	8 Monate
9	13.537.086.546.263.552	43 Jahre
10	839.299.365.868.340.224	2660 Jahre

Sicherheit in Abhängigkeit von der Passwortlänge

Quelle: <http://www.linuxbu.ch/pdf3/475-490.pdf>

Sicherheit

<i>Zeichensatz</i>	<i>Zeichen- zahl</i>	<i>Zahl der möglichen Passwörter</i>	<i>Zeitbedarf zum Knacken</i>
8-Bit ASCII	256	18.446.744.073.709.551.616	58.500 Jahre
7-Bit ASCII	128	72.057.594.037.927.936	228 Jahre
Buchstaben und Ziffern	62	218.340.105.584.896	8 Monate
nur Buchstaben	52	53.459.728.531.456	62 Tage
nur Kleinbuchstaben	26	208.827.064.576	6 Stunden
Wörter aus Wörterbuch	-	ca. 250.000	keiner

Sicherheit in Abhängigkeit vom Zeichensatz bei jeweils 8 Zeichen

Quelle: <http://www.linuxbu.ch/pdf3/475-490.pdf>

Sicherheit

Ein gutes Passwort...

- Möglichst lang, mindestens 8 Zeichen
- Verwendung von Klein- sowie Großbuchstaben, Ziffern und Sonderzeichen
- Bedeutungsloser Inhalt - keinesfalls Namen oder Wörter
- Anhängen oder Voranstellen von Ziffern und Sonderzeichen nicht ausreichend
- Modifizierte Passphrases als „Eselsbrücke“
- Regelmäßige Änderung
- Unterschiedliche Passwörter verwenden

Quellen:

http://www.bsi-fuer-buerger.de/schuetzen/07_0201.htm

<http://www.microsoft.com/switzerland/athome/de/security/privacy/password.msp>

J. Yan, A. Blackwell, R. Anderson, A. Grant: The memorability and security of passwords

Sicherheit

Problem Benutzer halten sich nicht an diese Vorgaben

Beispiel Kontaktmarkt “Flirtline“

- 100.000 Zugangsdaten kompromittiert
- 2,5% der Passworte beginnen mit Ziffernfolge '1234'
- starker Themenbezug, typische Vor- und Kosenamen

Ursache Ist der Benutzer schuld? >> Benutzbarkeitsprobleme

Ziel nicht den Mechanismus ändern, sondern wissensbasierte Authentifizierung anwendungsfreundlicher gestalten

[1] <http://lists.grok.org.uk/pipermail/full-disclosure/attachments/20060521/bda8d910/flirtlife.de-passwords-0001.zip>

Benutzbarkeitsprobleme

begrenzte Erinnerungsfähigkeit

- vs. bedeutungslose Inhalte
- vs. nicht-redundanter Passwörter
- vs. korrekte Wiedergabe / Rekonstruktion
- Vielzahl unterschiedlicher Anmeldenamen und Passwörter

mangelhaftes Wissen

- Benutzer fühlt sich von Bedrohungen nicht betroffen
- Unkenntnis
- Unterschätzter Einfluss auf das Gesamtsystem

Benutzbarkeitsprobleme

Wahrnehmung der Sicherheit

- Unverständnis
- Fehlende Akzeptanz
- Inkompatibel zu Arbeitseinsatz, Ineffektivität
- Vertrauenswürdigkeit der Daten wird nicht erkannt
- Chef zu wichtig für Authentifizierungsprozess >> „Ich darf alles!“
- System übertrieben sicher >> „da kann nichts passieren“
- Unsicheres System >> „da kommt es auf mich auch nicht an“
- Eigenes Verhalten unsicher >> „bisher ging es ja auch“

Benutzbarkeitsprobleme

Auswirkungen von Restriktionen

- Mindestlänge >> Redundanzen
- Zeichensatz >> Verwendung von Standard-Sonderzeichen
- Gültigkeit >> Variationen
- Komplexität >> Aufschreiben
- Multilogins >> Verwendung bestehender Passwörter

erzwungene Sicherheitsrichtlinien zur Steigerung der Sicherheit

haben gegenteilige Wirkung und **vermindern die Sicherheit** des Systems

Benutzbarkeit

Einflussfaktoren

- Anzahl verschiedener Accounts und Passworte
- Häufigkeit der Nutzung
- Kompatibilität mit Arbeitsorganisation
- Sensitivität der Informationen
- Kommunikation mit Systemadministratoren, Aufklärung, Schulung

Steigerung der Benutzbarkeit

Kommunikation zwischen Benutzer und Systembetreuer

- Aufklärung über sicherheitsrelevante Bedrohungen
 - Erläuterung der Auswirkungen
finanziell, rechtlich, auf das Gesamtsystem, für den Benutzer
 - Informationen über die Funktionsweise der Mechanismen
 - Vorbildfunktion der Administratoren
 - Mitteilung über versuchte Angriffe
- >> verbessertes **Sicherheitsbewusstsein** der Nutzer
- >> Need-to-know Prinzip

Steigerung der Benutzbarkeit

Nutzerverhalten beeinflussen

- Schulungen, Übungen und Beispiele anbieten
- Kontrolle
- Feedback und Ratschläge

Steigerung der Benutzbarkeit

Technische Implementierung

- Kombination mit alternativen Authentifizierungsmechanismen
- Einführung von Sicherheitsstufen
- Reduktion benötigter Passwörter:
 - >> Verwendung von Single-On-Systemen
 - >> Kontextbezogene Authentifizierung
- Einheitliche Anmeldenamen
- Restriktive Mechanismen vermeiden
- Graphische Passwörter – no total recall

Quellen:

Andrew Patrick, Human Factors of Security Systems: A Brief Review

Anne Adams, Martina Angela Sasse & Peter Lunt, Making Passwords Secure and Usable

Vielen Dank für Ihre Aufmerksamkeit