esse

ESSE Einführung in Security – VO 05: Identität, Authentifizierung, Zugriffskontrolle

Florian Fankhauser, Christian Schanes

INSO – Industrial Software
Institut für Information Systems Engineering | Fakultät für Informatik | Technische Universität Wien

Agenda

Identität

(Vergleiche Reality Check, „Identity Theft“, Dave Whamond, 16.01.2004)

Begriffe – 1/2

Identität Wer jemand ist

Authentisierung („authentication“) [0] Vorlage eines Nachweises zur Identifikation (z.B. Username/Passwort)

Authentifizierung („authentication“) [0] Überprüfung eines Nachweises zur Identifikation

Autorisierung („Authorization“) [0] Überprüfung, ob eine Person, IT-Komponente oder Anwendung zur Durchführung einer bestimmten Aktion berechtigt ist („Rechtetabelle“)

Begriffe – 2/2

Zutritt [0] Betreten von abgegrenzten Bereichen wie z.B. Räumen oder geschützten Arealen in einem Gelände

Zugang [0] Nutzung von IT-Systemen, System-Komponenten und Netzen

Zugriff [0] Nutzung von Informationen bzw. Daten

Quelle: [0] BSI: Glossar der Cyber-Sicherheit

Gründe für die Authentisierung/Authentifizierung

- Nachweis der Identität (Personen, Dienste, Komponenten)
- Voraussetzung für Kontrolle des Zutritts, Zugangs und Zugriffs
- Nachweis Zurechenbarkeit/Verantwortlichkeit
- *Identification is functionally dependent on authentication. Without authentication, user identification has no credability. Without a credible identity, neither mandatory nor discretionary security policies can be properly invoked because there is no assurance that proper authorizations can be made.* (Carlton et al.: Alternate Authentication Mechanisms)
- *Herstellung von Vertrauen zwischen zwei Kommunikationspartner:innen*

Herausforderungen bei der Authentisierung

- Valider Zutritt/Zugang soll einfach möglich sein
- Unberechtigte sollen zuverlässig vom Zugang abgehalten werden
- $\rightarrow$ Angreifer:innen reicht u.U. ein einzelner Account

Methoden der Authentisierung und Beispiele

- Wissen
  - Herkömmliche textuelle und graphische Passwörter
  - PINs
- Besitz
  - Tokens
  - Chipkarten
- Biometrisches Merkmal
  - Gesicht
  - Fingerabdruck
  - Stimme
  - Tippverhalten

Methoden der Authentisierung: Wissen

- Kennwörter wurden schon vor dem Einsatz in der Informationstechnik verwendet
  - Militär: Parole
  - Losungsworte
- Etablierte Methode zur Authentisierung
- Sicherheit abhängig von technischen und organisatorischen Faktoren
- „Verlust“ schwer oder erst zu spät erkennbar

Passwörter

- Passwörter werden häufig verwendet
- Auch in Form von Sicherheitsfragen
- Anzahl der Passwörter steigt

- Leicht zu merken vs. schwierig zu erraten
- Ausreichend große Basis an verfügbaren Zeichen, ggf. Klein- und Großbuchstaben, Ziffern, Sonderzeichen[1]
- Möglichst lange Passwörter
- Graphische Passwörter (Bildfolge, Punkte auf Bildern, Gesichter,...)
- U.U. Mindestlänge, Mindest-Vorkommen von einzelnen Zeichenklassen (Achtung bei 4 bzw. 6-stelligen Passwörtern, PINs)

[1] nicht zugelassene Zeichen ausschließen, falls nicht alles erlaubt...!

Weitere Regeln bei Verwendung von Passwörtern

- Keine Default-Passwörter verwenden
  - US CERT Alert TA13-175A: Risks of Default Passwords on the Internet
  - Default-Passwörter bei einem Confluence-Plugin
- Passwörter sollen nicht aufgeschrieben werden (v.a. nicht am Monitor, Keyboard etc.)
- Passwörter sollen von Benutzer:innen änderbar sein
- Anzahl der Versuche zur Passworteingabe beschränken (Achtung: Denial of Service)
- Prozess zur Änderung bei vergessenen Passwörtern
- Siehe BSI Grundschutz *ORP.4.A8 Regelung des Passwortgebrauchs* und weitere folgende Abschnitte, NIST Special Publication 800-63B

Fehlerhafte Passwort-Requirements

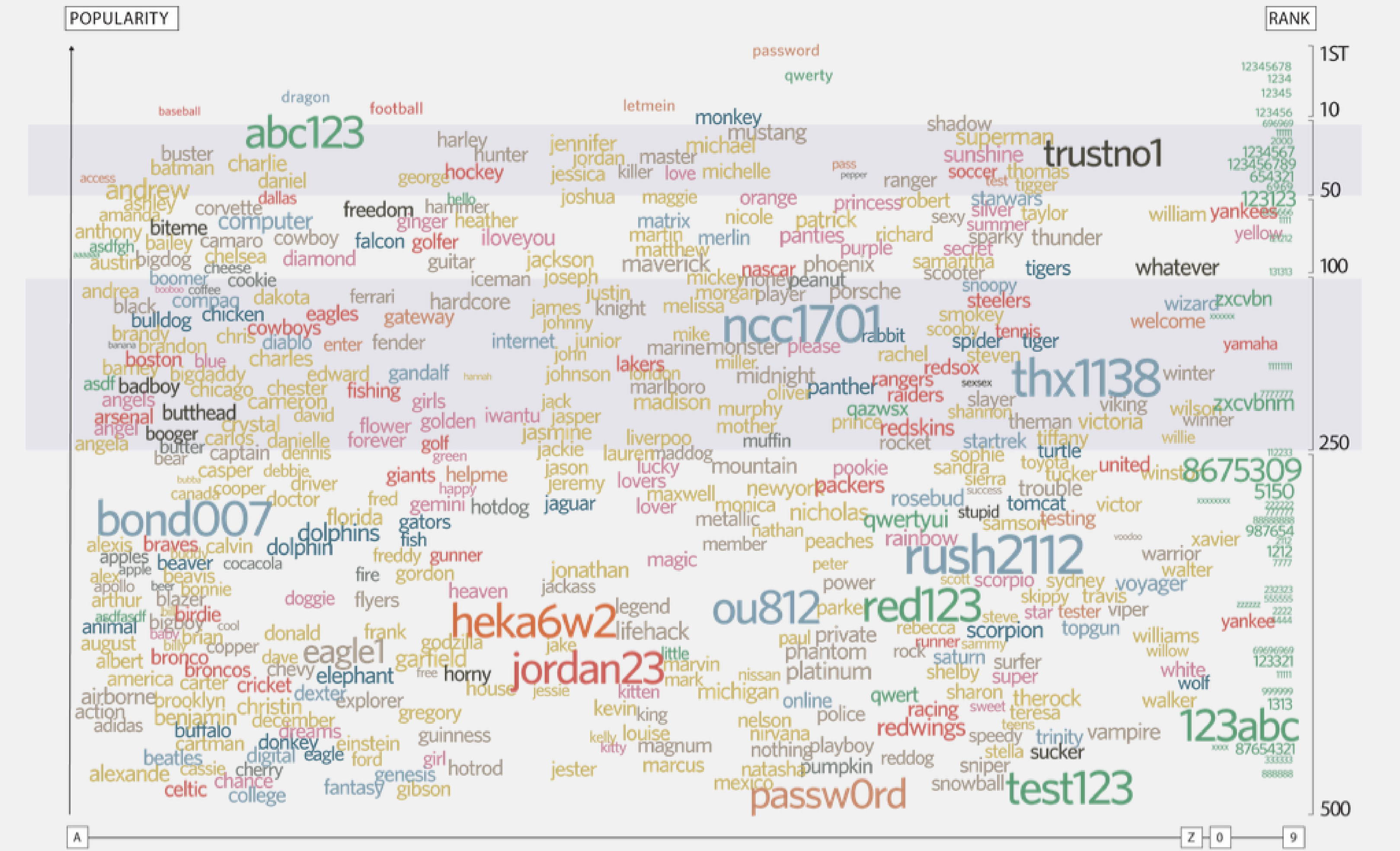
Your password must be at least 18770 characters and cannot repeat any of your previous 30689 passwords. Please type a different password. Type a password that meets these requirements in both text boxes.

(Vergleiche `https://web.archive.org/web/20050208013413/https://support.microsoft.com/kb/276304`)

Verwendung von schlechten Passwörtern

- Trotz aller Empfehlungen werden manche Passwörter häufig verwendet
- Ab und zu können aber auch schlechte Passwörter ausreichen – nicht alles muss gleich gut geschützt werden
- Sicherheitsbewusstsein stärken
- Beispiele für schlechte Passwörter
  - Familie (eigener Vorname/Nachname, Lebenspartner:innen, Kinder, Haustiere, Geburtsdatum,. . .)
  - Stars (Namen von Musiker:innen, Schauspieler:innen,. . .)
  - Username = Passwort
  - `123456`, `passwort`, `schatz`, `hallo`, `qwertz`, `abc123`

Top 500 Passwörter



http://www.informationisbeautiful.net/visualizations/top-500-passwords-visualized/

Design & Concept: David McCandless
Code & additional design: Omid Kashan

Sources: data breaches, Xato.net, TroyHunt.com
Data: http://bit.ly/KIB_Passwords

Zu komplexe Passwörter als Sicherheitsrisiko

(Vergleiche https://web.archive.org/web/20150624075117/https://ars.userfriendly.org/cartoons/?id=20071002)

Passwörter – Beispiele für Angriffe

- Raten, Default-Passwörter
- Brute Force (lokal, remote)
- Wörterbuch-Attacken (Traditionelle Wörterbücher, geleakte Passwörter, Domain-spezifisches Wissen,. . . ; Mutationen)
- Rainbow Tables
- Social Engineering, Phishing, Trojaner
- „Über die Schulter Schauen“, Wisch-Spuren auf Smartphones
- Script Files, Passwortdateien/Passwörter in Swap-Files
- Sniffing (Netzwerke, Bluetooth,. . .), z.B. auch Wireless-Tastaturen
- Preisgabe von Information: „Username/Passwort falsch“

Praxisbeispiel „Über die Schulter Schauen“

(Video)

Praxisbeispiel

Stärke von Passwörtern

Passwörter – Abwehrmethoden zu Angriffen

- Passwörter müssen am System sicher gespeichert werden, sie sollen nicht im Klartext gespeichert werden (Hash, Salt), Zugriffsschutz
- Eigene Hash-Algorithmen mit bestimmten Eigenschaften zur Verarbeitung von Passwörtern (siehe Provos und Mazières bzw. Password Hashing Challenge), z.B. `Argon2`, `bcrypt`
- Proaktive Passwort-Checker
- User-Training
- Lockout Mechanismen
- Passwort Wechsel bei Verdacht auf Security-Incidents
- Fehlanmeldungen/Letzte Anmeldung anzeigen
- Verwendung von Passwort-Safes mit automatisch erstellten Passwörtern

Umgang mit Passwörtern: Passwortbuch

Stärke von Passwörtern

(Vergleiche `https://xkcd.com/936/`)

Vertraulichkeit und Öffentlichkeit von Passwörtern

Sicherheitsfragen

(Vergleiche `http://bizarrocomics.com/`)

Methoden der Authentisierung: Besitz

- Physischer Gegenstand
- Verlust besser erkennbar als bei Passwörtern
- Erzeugung von Einmal-Passwörtern
  - Passwort auf Basis von aktueller Zeit
  - Passwort auf Basis eines Counters
- Immer wieder Schutz durch PIN/Passwort (z.B. Bankomatkarte)
- Physischer Schutz erforderlich
- Vorgaben für die Verwendung von PINs
- Kosten höher als bei Passwörtern

Chipkarten

- Besitz
- Anwendung z.B. mit kryptographischen Schlüsseln
- Gut: Privater Schlüssel verlässt die Chipkarte nicht
- U.U. geschützt durch PIN
- Gesamter Lebenszyklus relevant
- Einsatz z.B. Banken, Gesundheitswesen
- Angriffe
  - Social Engineering
  - Man in the Middle
  - Side Channel Attacken (Stromverbrauch, Rechenzeit,...)
  - Physikalisch (Temperatur, Spannung,...)

Methoden der Authentisierung: Biometrisches Merkmal

- Körperliches Merkmal
- Identifizierung von Menschen im zwischenmenschlichen Alltag
- Biometrische Merkmale sind schwer/nicht zu ersetzen
- Weitergabe von biometrischen Merkmalen schwer/nicht möglich
- Unterscheidung: Identifikation und Validierung
- Fehlerrate (FAR – False Acceptance Rate, FRR – False Rejection Rate)
- Akzeptanz von biometrischer Authentisierung
- Kosten höher als bei Passwörtern oder Token
- Ausprägung biometrischer Merkmale nicht bei allen Menschen gleich
  - Alternativen/Ausnahmen erforderlich

Angriffe bei biometrischen Merkmalen

- (Auch) Authentifizierung durch biometrische Merkmale nicht zu 100% sicher
- Stärken/Schwächen biometrischer Authentisierung werden oft vernachlässigt
- Spoofing (Hochauflösende Fotos (z.B. 31C3), Modellierung von (gefundenden) Fingerabdrücken,. . .)
  - Beispiel:
    Samsung Galaxy S5: Fingerabdrucksensor auch schon gehackt
- Replay Attacken
- Umgehen der Sensoren
- Brute Force
- Neuartige Angriffe durch KI

2-Faktor/Multifaktor-Authentifizierung

- Authentisierungsmethoden haben unterschiedliche Vor- & Nachteile
- Kein einziger, bester Weg für Authentisierung
- Je nach Einsatzzweck geeignetes Verfahren auswählen
- Kombination von Methoden
  - 2-Faktor-Authentifizierung, wenn 2 Methoden miteinander kombiniert werden
  - Multifaktor-Authentifizierung
- Siehe auch: Google aktiviert Zwei-Faktor-Authentifizierung für Accounts automatisch

FIDO2 – Fast IDentity Online 2

- FIDO2: Standard von FIDO-Allianz und W3C, breite Akzeptanz
- W3C WebAuthn als Web API für FIDO-Authentifizierung
- Spezifikation online verfügbar: `https://fidoalliance.org/`
- Grundidee von FIDO
  - Pro Site Erzeugung eigenes Private/Public Keypaar
  - Public Key kommt bei Registrierung zum Service, Verknüpfung mit Account
  - Bei Anmeldung wird Challenge (incl. Anfrage-Domain) zum Authenticator geschickt
  - Automatische Auswahl des richtigen Schlüssels
  - Signatur nach User-Interaktion
  - Nach erfolgreicher Signaturprüfung Anmeldung erfolgreich

FIDO2-Tokens

- FIDO2-Token als fehlerfreier, manipulationssicherer Computer
- Typisch: USB- und/oder NFC-Schnittstelle
- FIDO2-Token als Besitz-Faktor
- 5 Authenticator Levels
  - Von L1: Mobile App, Browser App, Android Keystore
  - Über L2: speziell abgesicherte Hardware
    - Erforderlich für A-Trust (ID Austria, Handysignatur, . . .)
  - Bis L3+: CC-zertifiziertes Secure Element
- Schadensbegrenzung bei Token-Verlust erforderlich

(Vergleiche Authenticator Certification Levels, A-Trust FIDO Tokens)

Passkeys als Beispiel für 2FA und Ersatz von Passwörtern

- Passkeys als Variante von FIDO2
- Ziele
  - Ersatz von Passwörtern
  - Höhere Sicherheit statt einfacher Passwörter
  - Schutz vor Phishing
- Übergreifende Verwendung von Passkeys über Devices und Plattformen hinweg
  - Verschlüsselte Speicherung der Passkeys in Clouds
- Beispiele für Unterstützer: Google, Apple, Microsoft

Zugriffskontrolle 1/2

- Zugang ist nun kontrolliert
- Zugriff sollen nur die berechtigten Akteure erhalten
- Unberechtigter Zugriff soll verhindert oder zumindest erkannt werden
- Zugriffskontrolle bedeutet Auditierung
- Zwei unterscheidbare Fälle für Angriffe
  - Angreifer:in hat Zugriff auf Binärdaten → Kryptographische Methoden erforderlich
  - Es existiert eine Schicht zwischen Angreifer:in und Binärdaten → Zugriffskontrolle

Zugriffskontrolle 2/2

- Umsetzung einer Sicherheitsstrategie (Security Policy)
- Verwendung von Zugriffskontrollmechanismen z.B. in
  - Betriebssystem
  - Datenbanken
  - Webserver
- Kernfrage der Zugriffskontrolle:
  - *Wer* darf auf *was* *wie* zugreifen.

Zugriffskontrollstrategie, Zugriffskontrollmodell

- Zugriffskontrollstrategie ist ein Regelwerk, das besagt was erlaubt/nicht erlaubt ist.
- Zugriffskontrollmodell ist ein Formalismus, um eine Zugriffskontrollstrategie zu beschreiben.
  - Verschiedene Zugriffskontrollmodelle für unterschiedliche Zugriffskontrollstrategien
  - Ein Modell soll einfach, ausdrucksstark, intuitiv, wartbar und umsetzbar sein.

Begriffe

Objekt [0] passiver, zu schützender Informationsträger

Subjekt [0] aktive Elemente, die im Auftrag von Anwender:innen Zugriffe auf Informationen ausführen

Zugriffsoperation Art, um auf ein Objekt zuzugreifen (read, write, execute,...)

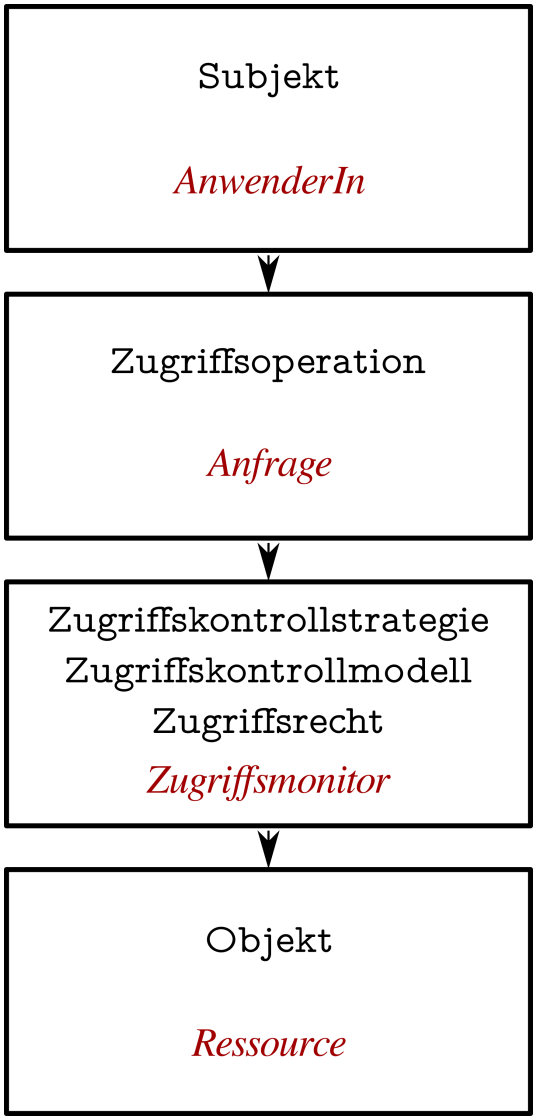
Zugriffsrecht Rechte für Zugriffe auf Dateien, Datenträger, Prozesse,...

Schutzdomäne Gruppierung von identischen Zugriffsrechten

Zugriffsmonitor setzt die Zugriffskontrollstrategie durch

Quelle: [0] siehe Einführung in die Informationssicherheit, hrsg. von H. Pohl, G. Weck

Zugriffskontrollmodell



Grundmodell der Autorisierung

- Ob für ein Subjekt s der Zugriff der Art a auf ein Objekt o zulässig ist, ergibt sich aus einer Funktion f, die das Ergebnis des 3-Tupels $(s;o;a)$, das *wahr* oder *falsch* sein kann, auswertet.
- Dabei gilt
  - $s \in S$, der Menge aller Subjekte
  - $o \in O$, der Menge aller Objekte
  - $a \in A$, der Menge aller möglichen Zugriffsarten

Zugriffsmatrix

Subjekt	Objekt				
	α	β	γ	δ	ϵ
a	0	0	1	0	1
b	1	1	1	1	0
c	0	0	0	0	1
d	0	1	1	1	0
e	1	1	0	1	0
f	0	1	0	0	1

- Zugriffsmatrix definiert die Zugriffsrechte
- Sichtweisen
  - Was darf ein Subjekt?
  - Was darf mit einem Objekt passieren?
- Umsetzung direkt als Matrix

  i.A. langsam, ineffizient

Beispiel für Gruppierung von Subjekten

Eigentümer	Der Eigentümer hat uneingeschränkte Zugriffsrechte.
Gruppe	Alle innerhalb einer speziellen Gruppe haben dieselben Zugriffsrechte, z.B. Lesen eines Objekts.
Jeder	Allen Usern in einem System können bestimmte Zugriffsrechte gegeben werden.

Discretionary Access Control (DAC)

- Ziel: Der/Die Besitzer:in legt Berechtigungen auf Objekte selbst fest
- Zugriff auf Objekte allein von der Identität abhängig
- Jedes Objekt hat einen Besitzer/eine Besitzerin
- Der/Die Besitzer:in kann Rechte für die Durchführung von Operationen an andere Benutzer:innen vergeben
- Verwaltung von Zugriffsrechten aufwändig (Zugriffsrechte auf Benutzer:innen-Ebene – Wechsel von Benutzer:innen)
- Aufwändig festzustellen welche Rechte bestimmte Benutzer:innen haben

Role-Based Access Control (RBAC)

- Ziel: Der Zugriff auf Objekte wird durch die Rolle festgelegt
- Benutzer:innen haben Rollen
- Von den Rollen hängen die Zugriffsrechte ab
- Eine Rolle ist eine Sammlung von Funktionen, die für eine Arbeit gebraucht werden (z.B. LVA-Leiter:in)
- Hierarchisches Rollenkonzept
- Benutzer:innen können mehrere Rollen haben, der Wechsel der Rollen ist möglich
- Rollen, die für eine Session gelten sollen, können aktiviert werden
- Rollen können andere Rollen ausschließen („Separation of Duty“)

Mandatory Access Control (MAC)

- Ziel: Zentrale Festlegung der (maximalen) Zugriffsrechte von Benutzer:innen
- Kontrolle des Informationsflusses
- Weitergabe von Rechten eingeschränkt möglich
- Objekte und Benutzer:innen haben Einstufungen (z.B. öffentlich, vertraulich, streng geheim)
- Benutzer:innen können lesend nur auf ein Objekt zugreifen, wenn ihre Einstufung mindestens der des Objekts entspricht
- Objekte können nur mit Einstufungen, die gleich- oder höherwertig der Einstufung des Benutzers/der Benutzerin ist, geschrieben werden
- Anwendung hauptsächlich im militärischen Bereich

(Weitere) Herausforderungen

- Concept of Least Privilege
- „Security stört nur“
- Identity and Access Management (IAM)
- Single Sign-On (SSO) (z.B. OAuth, SAML, OpenID...)
- Attribute Based Access Control (ABAC)
- Wie wird die Zugriffskontrolle administriert? Wer administriert? Wer zieht Berechtigungen zurück?
- Wo wird Zugriff kontrolliert? (Kontrolle von USB Stick am Rechner?)
- Technische Umsetzung
- Technische Separation von Subjekten

Praxisbeispiel

Stärke von Passwörtern

Quellen und weiterführende Literatur – 1/10

- Christian Brem: Slides INSO Security VU WS2006
- Bruce Schneier. *Secrets & Lies: Digital Security in a Networked World*. Wiley Publishing, Inc., Indianapolis, Indiana, 2004. ISBN 0-471-45380-3
- Bundesamt für Sicherheit in der Informationstechnik. BSI – IT-Grundschutz, 2021. `www.bsi.bund.de/grundschutz`
- Matt Bishop. *Introduction to Computer Security*. Pearson Education, Inc, 2003. ISBN 0-321-24744-2

Quellen und weiterführende Literatur – 2/10

- Hartmut Pohl und Gerhard Weck, (Hrsg.). *Einführung in die Informationssicherheit*. Sicherheit in der Informationstechnik. Oldenbourg, München, 1993. ISBN 3486220365
- Stephen F. Carlton, John W. Taylor, und John L. Wyszynski. Alternate Authentication Mechanisms. In *Proceedings of the 11th National Computer Security Conference*, Seiten 333–338, 1988. `https://csrc.nist.gov/CSRC/media/Publications/conference-paper/1988/10/17/proceedings-11th-national-computer-security-conference-1988/documents/1988-11th-NCSC-proceedings.pdf`
- Richard E. Smith. *Authentication: From Passwords to Public Keys*. Addison-Wesley, 2002

Quellen und weiterführende Literatur – 3/10

- Lawrence O'Gorman. Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, 91(12):2021–2040, Dezember 2003. ISSN 0018-9219. doi: 10.1109/JPROC.2003.819611
- Lynette I. Millett und Stephen H. Holden. Authentication and its privacy effects. *IEEE Internet Computing*, 7(6):54–58, November/Dezember 2003. ISSN 1089-7801. doi: 10.1109/MIC.2003.1250584
- Art Conklin, Glenn Dietrich, und Diane Walz. Password-based authentication: a system perspective. In *System Sciences, 2004. Proceedings of the 37th Annual Hawaii International Conference on*, Januar 2004. doi: 10.1109/HICSS.2004.1265412

Quellen und weiterführende Literatur – 4/10

- Xiaoyuan Suo, Ying Zhu, und G. Scott Owen. Graphical passwords: a survey. *21st Annual Computer Security Applications Conference*, Dezember 2005. ISSN 1063-9527. doi: 10.1109/CSAC.2005.27
- Roman V. Yampolskiy. Analyzing User Password Selection Behavior for Reduction of Password Space. In *Carnahan Conferences Security Technology, Proceedings 2006 40th Annual IEEE International*, Seiten 109–115, Lexington, KY, Oktober 2006. doi: 10.1109/CCST.2006.313438
- TeleTrust Deutschland e.V. Kriterienkatalog. Bewertungskriterien zur Vergleichbarkeit biometrischer Verfahren, 2006. `http://www.teletrust.de/publikationen/fachartikel/kriterienkatalog/`

Quellen und weiterführende Literatur – 5/10

- Jennifer G. Steiner, Clifford Neuman, und Jeffrey I. Schiller. Kerberos: An Authentication Service for Open Network Systems. In *Proceedings of the Winter 1988 Usenix Conference*, März 1988. `https://ftp.cs.toronto.edu/doc/athena/kerberos/usenix.PS`
- Florence Mwagwabi, Tanya McGill, und Michael Dixon. Improving Compliance with Password Guidelines: How User Perceptions of Passwords and Security Threats Affect Compliance with Guidelines. In *System Sciences (HICSS), 2014 47th Hawaii International Conference on*, Seiten 3188–3197, Januar 2014. doi: 10.1109/HICSS.2014.396
- William Burr, Hildegard Ferraiolo, und David Waltermire. NIST and Computer Security. *IT Professional*, 16(2):31–37, 2014. ISSN 1520-9202. doi: 10.1109/MITP.2013.88

Quellen und weiterführende Literatur – 6/10

- Eric Grosse und Mayank Upadhyay. Authentication at Scale. *Security Privacy, IEEE*, 11(1):15–22, Januar 2013. ISSN 1540-7993. doi: 10.1109/MSP.2012.162
- Barry Leiba. OAuth Web Authorization Protocol. *Internet Computing, IEEE*, 16(1):74–77, Januar 2012. ISSN 1089-7801. doi: 10.1109/MIC.2012.11
- Niels Provos und David Mazières. A Future-Adaptable Password Scheme. In *Proceedings of the USENIX Annual Technical Conference*. USENIX Association, 1999. `http://www.usenix.org/events/usenix99/provos/provos.pdf`
- `https://password-hashing.net/`
- Phraser-Tool: Passphrasen schneller knacken

Quellen und weiterführende Literatur – 7/10

- Heise Newsticker: Bericht: Apple-Support ermöglichte iCloud-Account-Übernahme
- Heise Newsticker: Preiswert Schlüssel knacken in der Cloud
- Scott Ruoti, Brent Roberts, und Kent Seamons. Authentication Melee: A Usability Analysis of Seven Web Authentication Systems. In *Proceedings of the 24th International Conference on World Wide Web*, WWW '15, Seiten 916–926, Republic and Canton of Geneva, Switzerland, 2015. International World Wide Web Conferences Steering Committee. ISBN 978-1-4503-3469-3. `http://dl.acm.org/citation.cfm?id=2736277.2741683`

Quellen und weiterführende Literatur – 8/10

- Simson Garfinkel, Gene Spafford, und Alan Schwartz. *Practical Unix & Internet security*. O'Reilly, 2003. ISBN 0596003234
- derStandard. Face ID: Zehnjähriger kann iPhone X seiner Mutter entsperren, 2017. `https://derstandard.at/2000067853581/Face-ID-Zehnjaehriger-kann-iPhone-X-seiner-Mutter-entsperren`
- Paul A. Grassi, Elaine M. Newton, Ray A. Perlner, Andrew R. Regenscheid, James L. Fenton, William E. Burr, Justin P. Richer, Naomi B. Lefkovitz, Jamie M. Danker, Yee-Yin Choong, Kristen K. Greene, und Mary F. Theofanos. NIST Special Publication 800-63B; Digital Identity Guidelines, Authentication and Lifecycle Management, Juni 2017

Quellen und weiterführende Literatur – 9/10

- Jürgen Schmidt. Passwörter: BSI verabschiedet sich vom präventiven, regelmäßigen Passwort-Wechsel, 2020. https://heise.de/-4652481
- Jimmy Kimmel Live, What is Your Password?, https://www.youtube.com/watch?v=opRMrEfAIiI
- MITRE, Brute Force: Password Spraying, https://attack.mitre.org/techniques/T1110/003/
- Das Ende des Passworts: Google startet Passkey-Unterstützung für Chrome und Android
- Die Handysignatur wird am 5. Dezember 2023 abgeschaltet

Quellen und weiterführende Literatur – 10/10

- Bundesamt für Sicherheit in der Informationstechnik. BSI TR-03107-1: Elektronische Identitäten und Vertrauensdienste im E-Government. Technischer Bericht, 2019. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR03107/TR-03107-1.pdf?__blob=publicationFile&v=1. Version 1.1.1
- Fefes Blog: Sun Mar 19 2023, Nachteile von Spracherkennung etc. durch KI

Zusammenfassung und Ausblick

- Identität, Authentisierung, Authentifizierung, Autorisierung
- Unterschiedliche Methoden zur Authentisierung
- Passwörter (Achtung, Passwortsicherheit im Lab!), Chipkarten, Biometrie
- Zugriffskontrolle
- Discretionary Access Control (DAC)
- Role-Based Access Control (RBAC)
- Mandatory Access Control (MAC)
- Zugriffskontrolle allein hilft jedoch bedauerlicher Weise auch nicht gegen alle Angriffe – IT-Sicherheit ist vielschichtig!

21.10.2023

Happy Global Encryption Day!

Vielen Dank!

https://establishing-security.at/