IT-SICHERHEIT UND DATENSCHUTZ

KAPITEL 3 - ZUGRIFFSKONTROLLE

buchmann@hft-leipzig.de

LERNZIEL UND AUFBAU DIESES KAPITELS

- Identifikation und Authentifikation
  - Wie lässt sich eine Identität bestätigen?
  - Welche Vor- und Nachteile haben die Varianten?
- Zugriffskontrolle
  - Aktuell etablierte Verfahren

- Lernziele
  - Sie können und Identifikation und Authentifikation abgrenzen.
  - Sie können den Konflikt zwischen Zugriffskontrolle und Nutzbarkeit eines Systems erklären und Lösungsvorschläge machen.
  - Sie können die vorgestellten Mechanismen zur Umsetzung der Zugriffskontrolle erklären und ihre Stärken und Schwächen diskutieren.

ZIELE DER IT-SICHERHEIT

- „Security triad“
  - **Vertraulichkeit**: Asset ist nur Autorisierten zugänglich
  - **Integrität:** Asset kann nur von Autorisierten modifiziert werden
  - **Verfügbarkeit**: Asset kann von Autorisierten genutzt werden

- ISO 7498-2 fügt hinzu
  - **Authentisierung**: Identität eines Senders wird überwacht
  - **Nichtabstreitbarkeit**: Sender kann nicht abstreiten, das eine Nachricht von ihm kam
- US Department of Defense fügt hinzu
  - **Auditierbarkeit**: Alle Aktionen mit dem Asset sind nachvollziehbar

IDENTIFIKATION UND AUTHENTIFIZIERUNG

WIE KANN MAN JEMANDEN IDENTIFIZIEREN?

- „Das blonde Mädel mit dem Tattoo, mit dem ich auf der Rolltreppe am Hauptbahnhof letzten Samstag Augenkontakt hatte“
- Personalausweisnummer #DE23948873984
- Der Besitzer des Fahrzeugs mit dem Kennzeichen „L AT-123“
- Der Nutzer des Webbrowsers, der folgenden Cookie speichert: „end_user_id:oeu1472024592717r0.221656711895419 7“

→ *Identifizierung hängt vom Anwendungskontext ab*

→ *Identifizierung kann ungenau oder zeitlich befristet sein*

PROBLEME MIT IDENTITÄTEN

- Manchmal kann jemand seine Identität nicht beweisen
  - Flüchtlinge aus Syrien warten nicht, bis ihnen die lokalen Behörden einen Pass ausstellen
- Es gibt gute Gründe, mehrere Identitäten anzunehmen
  - Eine Identität als fleißiger Arbeitnehmer, eine private gegenüber Facebook-Freunden, eine „brave“ gegenüber Verwandten
- Niemand sollte in der Lage sein, solche Identitäten zu verknüpfen
  - Arbeitgeber muss nicht wissen, was der Angestellte privat tut (s. Datenschutz-Kapitel)
- Es gibt gute Gründe, alte Identitäten zu vernichten
  - Eine Person ist Opfer eines Identitätsdiebstahls oder Stalkers, oder will ihr Leben ändern

DREI MÖGLICHKEITEN, EINE IDENTITÄT ZU BESTÄTIGEN

- Etwas, das die Person **weiß**
  - Passwörter, PIN-Nummern, Antworten auf Sicherheitsfragen wie “Was ist der Mädchenname Ihrer Mutter“
- Etwas, das die Person **ist**
  - Biometrische Merkmale wie Fingerabdrücke, Sprache, Gesichtserkennung, Blutgefäße in Netzhaut oder Hand
- Etwas, das die Person **hat**
  - Sicherheitstoken, Personalausweis, Schlüssel

→ lässt sich kombinieren, z.B. Geldautomat: PIN + Besitz der Karte

IDENTIFIKATION VS. AUTHENTIFIZIERUNG

IDENTIFIKATION VS. AUTHENTIFIZIERUNG

- Identitäten sind häufig *öffentlich*
  - Name einer Person, Email-Adresse, etc.
    z.B.: Email enthält Identität von Absender und Empfänger

- Authentifizierung sollte auf *privaten* Eigenschaften beruhen
  - Passwort, Fingerabdruck, Schlüssel, …

- Authentifizierung darf nicht für Identifizierung benutzt werden!
  - Wer ist die Person mit dem Passwort blabla38?
  - Welche Person hat den Fingerabdruck mit dem Hash 86AD100C?

  → *Ergebnis ist nicht zwingend eindeutig!*

KORREKTE UND INKORREKTE AUTHENTIFIZIERUNG

- **True positive**
  - System hat korrekte Authentifizierung akzeptiert
- **True negative**
  - System hat falsche Authentifizierung zurückgewiesen
- **False positive**
  - System hat falsche Authentifizierung akzeptiert
- **False negative**
  - System hat korrekte Authentifizierung zurückgewiesen

→ Wieviele False Positives/Negatives Sie erlauben, hängt von Ihrer Anwendung ab!

PASSWÖRTER

- Kategorie: Etwas, das die Person **weiß**
- Häufig genutzt, häufig falsch eingesetzt
- Wenn das System starke Passwörter erzwingt, finden Sie oft
  - ein Post-it irgendwo auf dem Schreibtisch, hinter dem Monitor, unter der Schreibtischunterlage oder unter der Tastatur
  - einen Zettel in der linken vorderen Ecke der obersten Schublade
- Wenn das System keine starken Passwörter erzwingt
  - 51% aller Passwörter bestehen aus weniger als 5 Buchstaben, alle klein geschrieben (s. Pfleeger: Security in Computing)
    → 265 = 11,881,373 Möglichkeiten

VERWENDUNG VON PASSWÖRTERN

- Verwendung als solche ist einfach
  - System fragt Nutzer nach Passwort, Nutzer gibt Passwort ein
  - System baut eine kryptographische Signatur vom Passwort
  - Wenn diese der gespeicherten Signatur entspricht, ist Nutzer authentifiziert
- Herausforderungen
  - Nutzung: Ein eigenes Passwort für jedes Asset ist unpraktisch
  - Enthüllung: Passwörter lassen sich ausspähen oder weitergeben
  - Zurückziehen: Wenn ein Passwort zurückgezogen wird, was passiert mit dem Asset, das gerade bearbeitet wird?
  - Verlust: Sichere Authentifizierung, wenn das Passwort vergessen wurde?

14.01.2021

MOBILE BUSINESS NEW YORK TIMES

Deutscher verliert Passwort zu riesigem Bitcoin-Vermögen

Ein Programmierer in San Francisco hat der „New York Times“ zufolge nur noch zwei Versuche, um das vergessene Passwort eines Bitcoin-Vermögens zu erraten, das aktuell mehr als 200 Millionen Dollar wert ist.

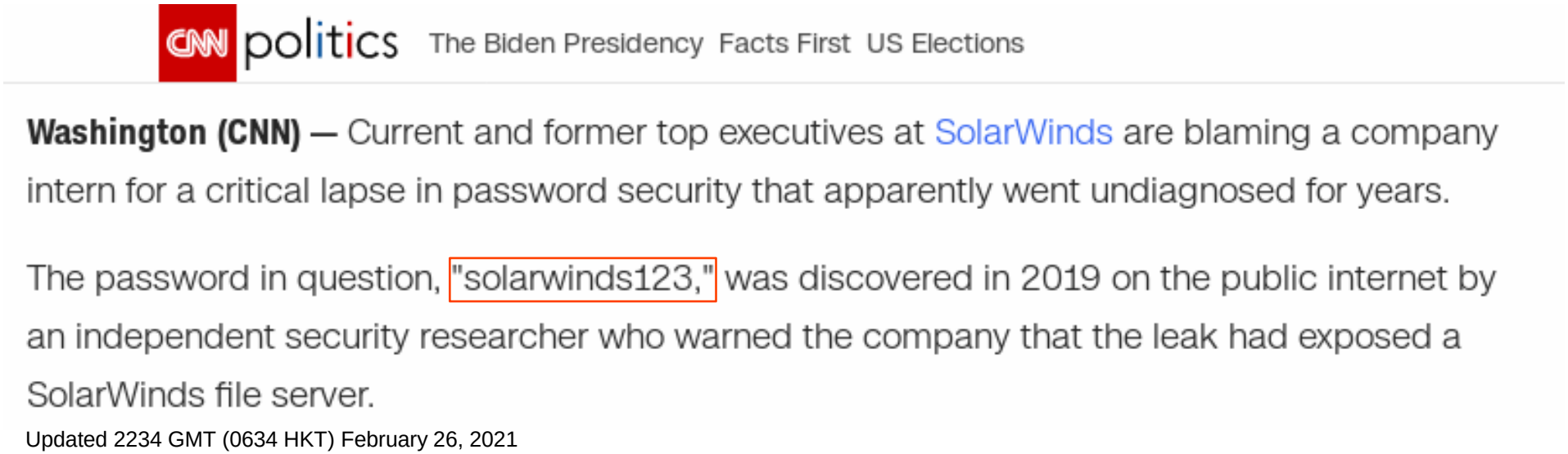
ANGREIFBARKEIT VON PASSWÖRTERN

- Passwörter werden als kryptographische Signatur gespeichert
- System könnte eine zeitlang blockieren, wenn ein Nutzer mehrmals hintereinander ein falsches Passwort eingegeben hat
  - Angreifer kann auf diese Weise nicht Millionen von Passwörtern pro Sekunde ausprobieren
  - Aber: Kann als Denial of Service gegen Nutzer eingesetzt werden
- Kryptographische Signaturen müssen geheim bleiben
  - Wenn Angreifer Signaturfunktion kennt, kann er sonst auf seinem Rechner tatsächlich alle Passwörter ausprobieren
- 8 Zeichen aus {a-z|A-Z|0-9} erlauben 62^8 = 218 Billionen Kombinationen
  - Sicher genug?
  - Zum Vergleich: Duden enthält ca. 18 Mio. Wörter (Stand 2020)

218 BILLIONEN KOMBINATIONEN REDUZIEREN

- Ablauf beim Passwörter-erraten
  1) kein Passwort
  2) dasselbe wie der User Account im System
  3) ähnlich zum Vor- oder Nachnamen des Nutzers
  4) gebräuchliches Wort + irgendein einfaches Muster (z.B. „password123“, „qwerzt-geheim“)
  5) im Wörterbuch der Muttersprache des Nutzers
  6) im Wörterbuch in einer Fremdsprache
  7) im Wörterbuch mit einfachen Ersetzungen (0 → O, S → 5 etc.) with Großbuchstaben („PaSsWorT“)
  8) alle erlaubten Kombinationen aus Buchstaben/Zahlen
  9) alle erlaubten Kombinationen von (Sonder-)Zeichen

SOWAS NENNEN DIE MEDIEN „HACKERANGRIFF“ :-/



CNN politics The Biden Presidency Facts First US Elections

Washington (CNN) — Current and former top executives at SolarWinds are blaming a company intern for a critical lapse in password security that apparently went undiagnosed for years.

The password in question, "solarwinds123," was discovered in 2019 on the public internet by an independent security researcher who warned the company that the leak had exposed a SolarWinds file server.

Updated 2234 GMT (0634 HKT) February 26, 2021

Anmerkung: SolarWinds stellt Security-Tools für Datenbank- und Netzwerküberwachung her. Passwort betraf Update-Server, daraufhin wurden Updates mit Trojanern an alle Kunden ausgeliefert. Passwort vom Praktikanten gesetzt.

DEN PASSWORTSCHUTZ UMGEHEN

- Zum Beispiel durch
  - erraten der Antworten auf die Sicherheitsfragen
  - physischen Zugriff auf das Gerät

SICHERE PASSWÖRTER

- Postillon, 2014:

IT-Experten küren Mb2.r5oHf-0t zum sichersten Passwort der Welt

Hamburg (dpo) - Gehackte Accounts, Sicherheitslücken, E-Mail-Datenklau: Immer mehr Menschen machen sich berechtigterweise Sorgen über ihre Passwortsicherheit. Doch damit dürfte bald Schluss sein. Der Chaos Computer Club (CCC) hat heute Mb2.r5oHf-0t offiziell zum sichersten Passwort der Welt gekürt. Zuvor waren in ausgiebigen Testreihen alle gängigen Passwort-Knack-Programme an der ausgeklügelten Zeichenfolge gescheitert.

"Die Zeichenfolge Mb2.r5oHf-0t ist einfach makellos: Sie beinhaltet Großbuchstaben, Kleinbuchstaben, Satzzeichen und Ziffern – ohne dass an irgendeiner Stelle zwei Zeichen der gleichen Kategorie aufeinanderfolgen würden", schwärmt Malte Winkler vom CCC. "Deshalb kann man mit Fug und Recht sagen: Wer sich mit Mb2.r5oHf-0t schützt, der ist sicher. Garantiert."

BIOMETRIE

- Kategorie: Etwas, das die Person **ist**

- Biologische Merkmale basierend auf den Eigenschaften des Körpers
  - Fingerabdruck
  - Geometrie der Handfläche
  - Blutgefäße in Netzhaut, Finger, Hand, Gesicht
  - Handschrift, Timing beim Tippen auf der Tastatur
  - Stimme
  - Gesichtsform, Anordnung von Nase, Mund, Augenbrauen
  - …

EIGENSCHAFTEN VON BIOMETRISCHEN MERKMALEN (1/2)

- Unveränderlich!
  - Anders als beispielsweise Passwörter
  - Öffentliche biometrische Merkmale sind für immer „verbrannt“
- Sensibel!
  - Tiefer Eingriff in die Privatsphäre des Nutzers
  - Zur Authentifizierung gemessene Merkmale können zusätzliche sensible Informationen enthalten
- Offen für Manipulationen!
  - Fingerabdruck auf Gummifinger, Aufzeichnung der Stimme, Foto

EIGENSCHAFTEN VON BIOMETRISCHEN MERKMALEN (2/2)

- Anteil der False positives kann sehr hoch sein
  - Schwellwert, ab wann gemessene Eigenschaften übereinstimmen
  - Es gibt immer Leute, die ein Merkmal nicht nutzen können
    - Unlesbare Fingerabdrücke, fehlende Augen/Gliedmaßen, stumm, …
  - Sicherheitsbeweis unmöglich
    - Weder Nutzer noch Betreiber kann *beweisen*, dass System Sicherheitskriterien erfüllt
    - nur statistische Aussagen durch Nutzerstudien
  - *Niemals Authentifizierung für Identifizierung nutzen!*

The finger pads of a person with adermatoglyphia are entirely smooth. (Photo by Sprecher et. al.)

TOKEN-BASIERTE AUTHENTIFIZIERUNG

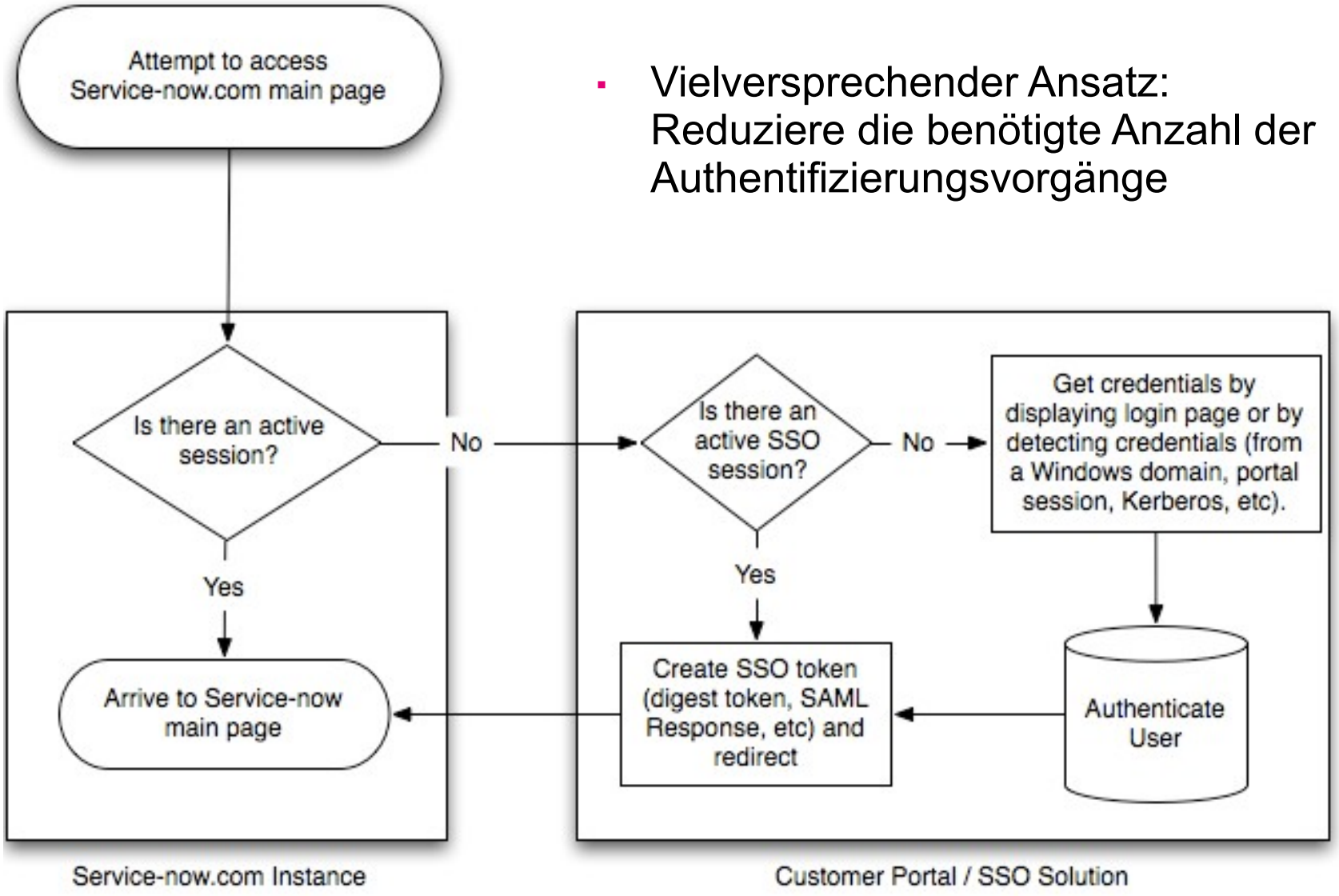
- Kategorie: Etwas, das der Nutzer **hat**
- **Passive Token**
  - Schlüssel, Ausweise, etc.
- **Aktive Tokens**
  - Lassen sich digital auslesen
    e.g., RFID-chip, EC-Karte
- **Statische Tokens**
  - Unveränderliche Daten
- **Dynamische Token**
  - Daten ändern sich über die Zeit

→ *Wo wäre ein PIN/TAN-Verfahren in diesem Schema?*

BENUTZERFREUNDLICHKEIT VS. SICHERHEIT

- Wird die Sicherheit übertrieben, suchen die Nutzer andere Wege

SINGLE SIGN-ON



- Vielversprechender Ansatz: Reduziere die benötigte Anzahl der Authentifizierungsvorgänge

ZUGRIFFSKONTROLLE

ZUGRIFFSKONTROLLE

Wiederholung

- Subjekt, Art des Zugriffs, Objekt und Regel

Subjekt
(Wer möchte zugreifen)

Art des Zugriffs
(Wie soll das passieren)

Objekt
(Was wird zugegriffen)

Regel:
f(Wer + Was + Wie) → {Ja|Nein}

EFFEKTIVE ZUGRIFFSKONTROLLE

- Prüfe **jeden** Zugriff
  - Ein einmal autorisiertes Subjekt muss nicht notwendigerweise auch später noch Zugriffsrechte haben (*Was ist mit Sigle Sign-on?)*
- Vergebe die **minimale Menge** an Privilegien
  - Ein Subjekt sollte Zugriff auf die kleinste Menge an Assets haben, die notwendig sind um die gestellte Aufgabe zu erfüllen (*Least Privilege*)
- Prüfe, was eine **akzeptable Nutzung** ist
  - Eine Zugriffsberechtigung ist eine ja/nein-Entscheidung
  - Wie müssen Zugriffsberechtigungen aussehen, damit ein Subjekt nur das mit einem Asset tun kann, was es tun darf? *(Integritätssicherung)*

AUCH ZUGRIFFSRECHTE ÄNDERN SICH MIT DER ZEIT!

- Rechte müssen *immer* und am besten *sofort* an Änderungen in der Unternehmensstruktur angepasst werden

  - Größte Herausforderung für Zugriffsregeln überhaupt

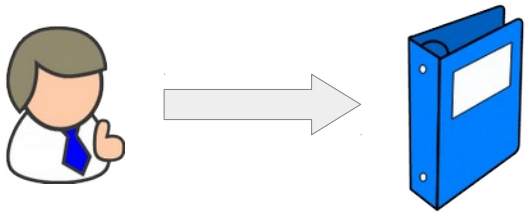
    Wer hat alles vergessene Schlüssel von früheren Tätigkeiten/Ausbildung/Vereinen etc. in der Schublade?

    Wer hat alles vergessene Accounts von früheren Tätigkeiten/Ausbildung/Vereinen etc., die er nicht mehr braucht?

UMSETZUNGSOPTIONEN FÜR ZUGRIFFSKONTROLLE

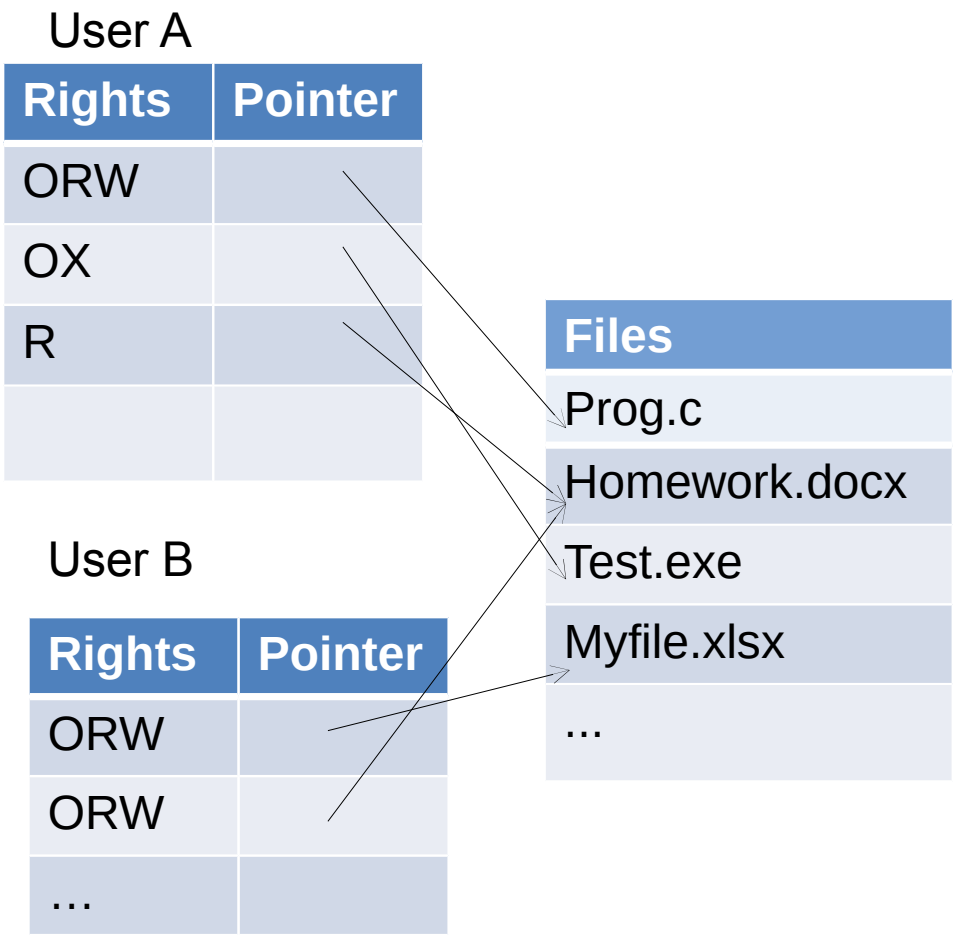
- Im Folgenden
  (Beispiel Dateizugriff, geht aber im Prinzip für jede Art Asset)

  - Access Control Directory
  - Access Control List
  - Access Control Matrix
  - Access Token (auch bekannt als Capability)
  - Procedure-Oriented Access Control
  - Role-based Access Control



ACCESS CONTROL DIRECTORY

- Ein User ist der Besitzer
- Jeder User bekommt ein Verzeichnis mit einer Auflistung der Zugriffsrechte
  (O: Owner; R: Read; W: Write; X: Execute)
- Schwerwiegende Nachteile
  - Wie herausfinden, wer alles Zugriff auf ein Objekt hat?
    → *Rechte entziehen ist teuer*
  - evtl. riesige Verzeichnisse
  - Integrität der Verzeichnisse *jederzeit* garantieren?
- *Sollte nicht mehr benutzt werden*



ACCESS CONTROL MATRIX

- Eine Matrix speichert alle Zugriffsrechte
  - Spalten: Subjekte
  - Zeilen: Objekte
  - Zellen: Berechtigungen
- Zugriffsrechte finden ist etwas effizienter
- Matrix wird evetuell riesig
- Integrität der Matrix garantieren?
- *Sollte nicht mehr benutzt werden*

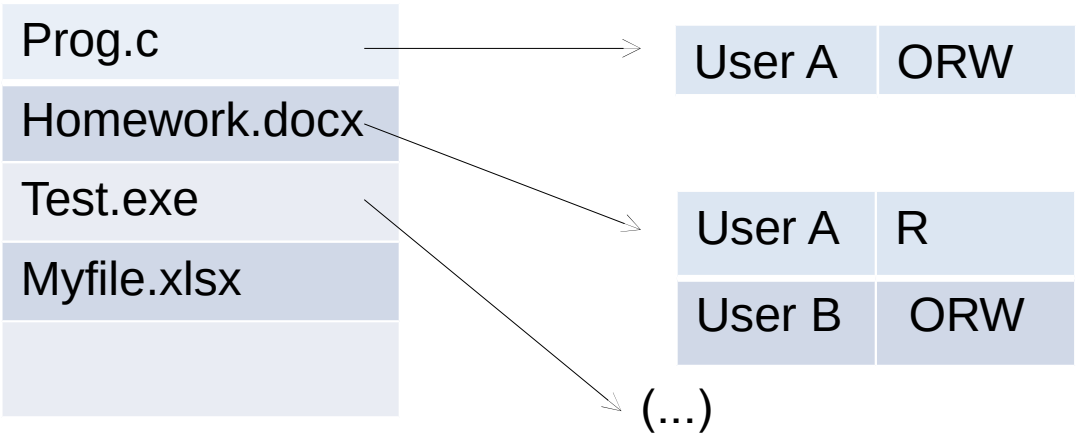
Name	User A	User B
Prog.c	ORW	
Homework.docx	R	ORW
Test.exe	OX	
Myfile.xlsx		ORW
…		

ACCESS CONTROL LIST (ACL)

- Liste {(user|group|all), permissions} wird an jedes Objekt angehängt
  - EINE Liste enthält also alle Rechte dieses Objekts

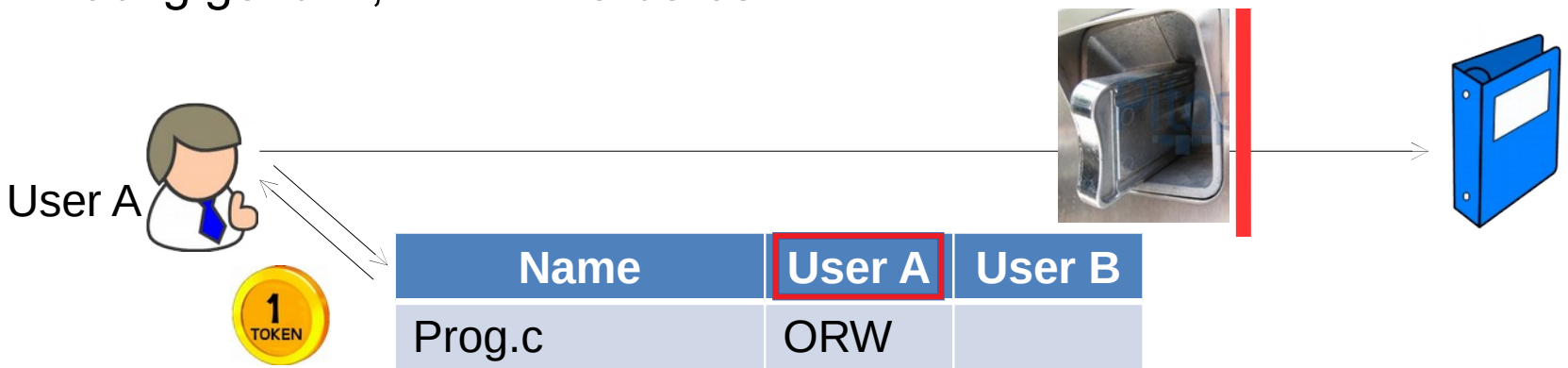
- Effizient zu verarbeiten, flexibel Einsetzbar
- Integritätsprobleme einer Liste bleiben auf ein einzelnes Objekt begrenzt
- Klein, wenn man die Listen nur die Berechtigungen speichern lässt, die über Standardrechte hinausgehen

- Wird heute oft benutzt
  - Dateisysteme von Windows, Unix, Linux, Mac OS, ...



ACCESS TOKENS

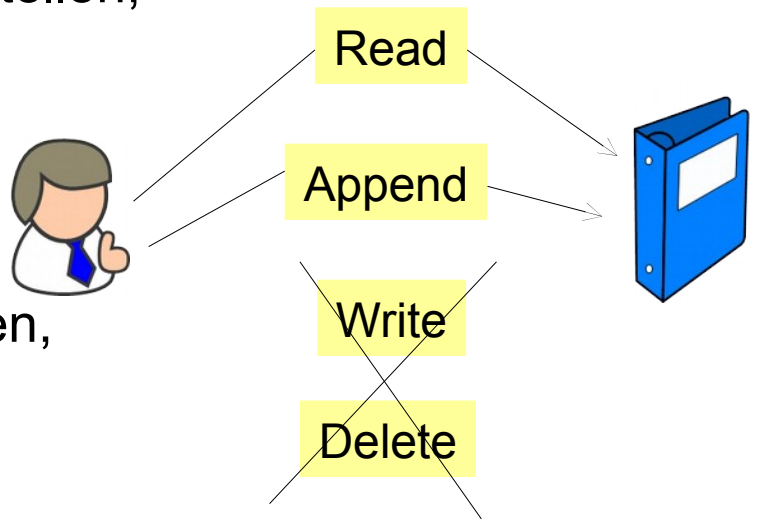
- Nutzer holt sich ein signiertes Token vom System, das das Recht bescheinigt, auf ein Objekt auf eine bestimmte Art zugreifen zu dürfen
  - Access Token wird auch als „capability“ bezeichnet
  - Je nach Implementierung ein- oder mehrmals verwendbar, weitergebbar
  - Gut parallelisierbar: Sicherheitssystem muss nur authentifizieren und Rechte speichern, Dienst muss nur Gültigkeit des Tokens prüfen
  - Flexibel einsetzbar, aber Kommunikationsoverhead
  - Häufig genutzt, z.B. in Kerberos



Name	User A	User B
Prog.c	ORW	
Homework.docx	R	ORW
Test.exe	OX	
Myfile.xlsx		ORW

PROCEDURE-ORIENTED ACCESS CONTROL

- Auf Objekte wird nur über definierte Prozeduren zugegriffen
  - Prozeduren wie „schreiben“, „lesen“, „wert um 10 erhöhen“, ...
  - Kein direkter Zugriff durch den Nutzer
- Zugriffskontrolle wird über Prozeduren erledigt
  - Objektorientierte Kapselung des Zugriffs
  - Nur erlaubte Zugriffsmöglichkeiten im System
  - Zugriff über vertrauenswürdige Schnittstellen, es kann keiner „von außen“ kommen
- Eher langsamer Zugriff, da Objekt nicht direkt manipulierbar
- Oft in Datenbanken genutzt (z.B. Schreibzugriff auf Datenobjekt verboten, aber Zugriff auf Stored Procedures erlaubt, welche die Änderungen vornehmen)



ROLE-BASED ACCESS CONTROL (RBAC)

- Zugriffsrechte an Rollen gebunden, Rollen werden Nutzern zugewiesen
  - Rollen können Administrator, Audio, Video, User, etc. sein
  - Jeder Nutzer kann viele Rollen haben

- Passt gut in große, strukturierte Unternehmen
  - Nutzer wechselt → Rolle „Abt. A“ entziehen, Rolle „Abt. B“ geben
  - Abteilungen ändern sich → Zugriffsrecht X der Rolle „Abt. A“ entziehen
  - Effizient implementierbar, Integritätssicherung kein Problem

- Eher unflexibel bei vielen spezialisierten Nutzern
  - Eventuell viele Rollen, die jeweils nur einem Nutzer zugeordnet sind
  - „Überlappende“ Rollen müssen von Hand vermieden werden (Rolle A gibt Zugriffsrecht auf X,Y, Rolle B gibt Zugriffsrecht auf Y,Z)

- Heute sehr häufig genutzt

ABSCHLUSS

ZUSAMMENFASSUNG

- Identifikation und Authentifizierung sind die Grundlage für jeden Mechanismus zur Absicherung der Assets
  - Nutzerakzeptanz ist ein wichtiger Sicherheitsfaktor!
    Aufwand und andere Seiteneffekte müssen berücksichtigt werden
- Niemals Identifikation (*öffentliche Merkmale*) und Authentifizierung (*private Merkmale*) mischen
  - Also nicht beispielsweise jemanden anhand seines Fingerabdrucks identifizieren UND authentifizieren
- Verschiedene Implementierungen von Zugriffskontrollmechanismen
  - Jeder Ansatz hat spezifische Vor- und Nachbteile

MÖGLICHE PRÜFUNGSFRAGEN

- Beschreibe für jeden Zugriffskontrollmechanismus, auf welche Weise und mit wieviel Aufwand (a) das System feststellen kann, ob jemand Zugriffsrechte für ein Objekt besitzt, (b) neue Zugriffsrechte für ein Subjekt hinzugefügt werden können, (c) Zugriffsrechte eines Nutzers zurückgezogen werden können, (d) neue Objekte mit Standard-Zugriffsrechten für alle Nutzer hinzugefügt werden können.

- Beschreiben Sie eine Situation, in der ein einfaches, aber leicht zu merkendes Passwort als Zugriffsschutz angemessen ist.

- Nennen Sie drei Gründe, warum Nutzer biometrische Zugriffskontrollverfahren ablehnen könnten.

- Warum haben wir davon abgeraten, Verfahren zur Authentifizierung auch gleich für die Identifizierung zu verwenden?

LITERATUR

- Pfleeger, Charles P. et al.: Security in Computing, *Prentice Hall,* 2015

- Eckert, Claudia. IT-Sicherheit: Konzepte-Verfahren-Protokolle. *Walter de Gruyter*, 2018

  (Die Auflage ist für Grundlagenkapitel egal, falls Sie eine alte Version besitzen oder als PDF im Netz finden)