Computersystemsicherheit – Übungsblatt Nr. 5

Marc Fischlin, Jacqueline Brendel, Christian Janson
TU Darmstadt, 21. Dezember 2018

Gruppenübung. Die Übungsaufgaben in diesem Bereich sind Gegenstand der Übungen in der Woche vom 21.01.2019 – 25.01.2019.

Aufgabe 1 (Verständnisaufgaben).

a) Was ist ein false positive Fehler und false negative Fehler?

b) Nennen Sie jeweils drei Vor- und Nachteile von Single Sign-On Diensten.

c) Erklären Sie kurz das Konzept was hinter Discretionary Access Control (DAC) steckt.

d) Erklären Sie kurz das Konzept von Mandatory Access Control (MAC) und zeigen Sie Unterschiede zu DAC.

e) Was ist eine Access Control List?

f) Wann gehört ein Dienst zu einem von einem Kerberos-Server verwalteten sogenannten *Realm*, d.h. zu den Diensten, die Tickets des zugehörigen Ticket Granting Servers akzeptieren?

g) Wozu wird der Authentication Server bei Kerberos benutzt?

h) Kann man sich seine IP-Adresse frei einstellen / wählen? Kann man seine MAC-Adresse frei einstellen / wählen?

i) Was ist ARP-Spoofing?

j) Kann man sich per ARP-Spoofing als Man-in-the-Middle zwischen eine Webseite im Internet und einem anderen Benutzer im Internet positionieren? Begründen Sie.

k) Welche Gegenmaßnahme gibt es gegen DNS Spoofing?

l) Was ist der Unterschied zwischen einem SYN-Flood-Angriff und einem SYN-ACK-Flood-Angriff?

m) Was sind Firewalls und wofür werden sie eingesetzt?

n) Erklären Sie kurz die Grenzen von zustandslosen Firewalls und geben Sie den Hauptunterschied zu zustandsbasierten Firewalls an.

o) Wie ist es zustandsbasierten Firewalls möglich SYN-Flooding zu erkennen und abzuwehren?

Aufgabe 2 (Zugriffsmatrix). Auf der Hauptbrücke eines Raumschiffes gibt es verschiedene Konsolen für die Kontrolle der unterschiedlichen Schiffssysteme. Die verschiedenen Mannschaftsmitglieder haben unterschiedliche Rechte an den Konsolen. Nehmen Sie folgendes an:

- Mannschaftsmitglieder: Captain (C), First Officer (FO), Science Officer (SO), Tactical Officer (TO), Helm Officer (HO), Ensign (E)
- Konsolen: Navigation Console (NC), Sensor Console (SC), Tactical Console (TC), Self-Destruction Console (DC)
- Zugewiesene Rechte:
  - r: (Lese-)Zugriff auf Konsole
  - w: Programmierung der Konsole
  - x: Ausführen von Aktionen auf der Konsole
  - rwx: Vollzugriff auf Konsole
  - rwx: Befehligen eines anderen Mannschaftsmitglieds
- C darf alles und auch alle anderen Mannschaftsmitglieder befehligen.
- FO darf alles und auch alle anderen Mannschaftsmitglieder außer C befehligen.
- SO hat Vollzugriff auf SC.
- TO hat Vollzugriff auf TC, r-Recht an SC und darf HO befehlen.
- HO hat Vollzugriff auf NC und r-Recht an SC.
- E nimmt von allen anderen Mannschaftsmitgliedern Befehle entgegen.

a) Legen Sie mit Hilfe des Zugriffsmatrix-Modells die Zugriffsrechte der beteiligten Mannschaftsmitglieder zu den unterschiedlichen Objekten und Subjekten fest.

b) Welche Probleme treten bei diesem Modell auf wenn eine statische Zugriffsmatrix verwendet wird und wie würden Sie vorgehen, um diese Probleme zu verhindern?

Aufgabe 3 (Bell-LaPadula Modell). Sie gründen ein IT-Startup und wissen bereits im Vorfeld, dass Sie firmeninterne Zugriffsregeln festlegen möchten um bestimmten Mitarbeitern den Zugriff auf klassifizierte Dokumente zu verwehren. Aus der in Ihrem Studium besuchten Veranstaltung Computersystemsicherheit erinnern Sie sich an das Bell-LaPadula-Modell.

Als Beispiel aus dieser Veranstaltung besitzen Sie die Access Control Matrix (ACM), die wie folgt aussieht:

	Geschenkeliste	**Kuchenrezept**	**Streiche**
Osterhase	`read, write`	`read`	`execute`
Weihnachtsmann	`read, execute`	`read, execute`	`write`
Zwerg	`write`	`read, write, execute`	`execute`

a) Sie möchten diese ACM zu Ihrem Zwecke nutzen und nur minimal verändern. Für Ihr Unternehmen definieren Sie drei Rollen:

- Personalmanager (PM)
- CEO (CEO)
- Programmierer (PROG)

und drei Objekte:

- Gehaltsabrechnung (GA)
- To-do-Liste (ToDo)
- Besorgungsliste (BL)

Welche vorhandenen Subjekte bzw Objekte müssen sie in der gegebenen Matrix durch Ihre Rollen bzw Objekte ersetzen, so dass folgende Regeln gelten, ohne dass Sie die bereits eingetragenen Zugriffsrechte verändern müssen?

Regeln:

- To-Do-Listen werden nur vom CEO bearbeitet (execute)
- Der CEO schreibt (write) Besorgungslisten nur, kümmert sich aber nicht weitere darum
- Der Personalmanager darf als einziger Gehaltsabrechnungen schreiben (write), alle anderen düren sie mindestens lesen (read)

b) Sie übernehmen auch die unten gegebenen **classification**- und **clearance**-Zuordnung Ihrer früheren Vorlesung und übertragen sie 1:1 auf Ihre ACM

- **classification**(Geschenkeliste) = 6
- **classification**(Kuchenrezept) = 4
- **classification**(Streiche) = 8
- **clearance**(Osterhase) = 6
- **clearance**(Weihnachtsmann) = 10
- **clearance**(Zwerg) = 4

(i) Mit welchen Mitteln können Sie anhand der ACM entscheiden, ob Vertraulichkeit garantiert ist?

(ii) Entscheiden Sie, ob Ihre ACM Vertraulichkeit garantiert.

c) Ändern Sie entweder genau einen **clearance**- oder genau einen **classification**-Wert, sodass ihre ACM Vertraulichkeit garantiert. Die **clearance**- und **classification**-Funktion nehmen beide Werte aus der Menge $\{1, .., 10\}$ an.

d) Welche Sicherheitsklassifikation $sb(O)$ muss ein Objekt O haben, so dass ein Subjekt S mit einer Sicherheitsklasse $sb(S) = x$ sowohl lesend, als auch schreibend darauf zugreifen kann?

Aufgabe 4. Neben dem vollautomatischen Lösen von CAPTCHAs durch Texterkennungs- und anderen Maschinenlernalgorithmen, hat sich auch ein Markt für das halbautomatische Lösen von CAPTCHAs etabliert. Es gibt Webseiten, auf denen man CAPTCHAs lösen kann um Punkte zu sammeln. Anschließend kann man die Punkte ausgeben, um sich automatisch von anderen Benutzern CAPTCHAs lösen zu lassen. Das Lösen eines CAPTCHAs kostet 10 Punkte. Löst man selbst ein CAPTCHA, erhält man 7 Punkte. Man kann auch Punkte für Geld kaufen oder sich Geld auszahlen lassen für Punkte. In unserem Beispiel (Zahlen von einer konkreten Webseite) kostet das Lösen von 4000 CAPTCHAs 5 €. Dies ist der kleinstmögliche Block an Punkten, den man kaufen kann. Umgekehrt kann man sich für das Lösen von 1000 CAPTCHAs jeweils 0,50 € auszahlen lassen (jedoch erfolgt die Auszahlung erst sobald mindestens 10 € zusammengekommen sind). Dadurch werden Entwickler motiviert, diesen Prozess immer einfacher zu machen, bis hin zur völligen Automatisierung auch schwieriger CAPTCHAs. Die Webseite bietet zahlreiche APIs für verschiedene Programme, Webseiten und Programmiersprachen an.

a) Eine Zeitschrift führt eine Onlineumfrage durch. Der Gewinner der Umfrage erhält 20000 € Spenden. Ihr Favorit ist auf dem 6. Platz. Er hat 6000 Stimmen. Die Umfrage wird angeführt mit 17353 Stimmen. Um sich vor Manipulationen zu schützen, setzt die Zeitschrift CAPTCHAs ein. Wie viel würde es kosten, mithilfe des oben genannten Services ihren Favoriten auf Platz 1 zu heben?
Angenommen ihr Favorit gewinnt nach dieser Investition und sie profitieren selbst von dem Gewinn. Wie groß ist die Gewinnspanne?

b) Kann dieser Angriff auffallen? Begründen Sie.

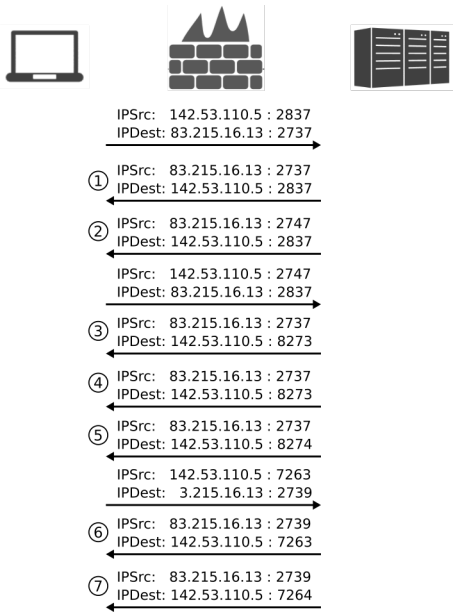
c) Angenommen man hat sich Punkte durch das Lösen von CAPTCHAs verdient und will diese Punkte nun einsetzen, um eigene CAPTCHAs automatisch lösen zu lassen. Wie viele gelöste CAPTCHAs kann man sich von diesen Punkten kaufen, im Verhältnis zu den CAPTCHAs, die man selbst lösen musste, um an die Punkte zu kommen.

d) Wie viel verdient man als hauptberuflicher CAPTCHA-Löser pro Stunde? (Nehmen Sie dafür an, dass man durchschnittlich 30 Sekunden für das Lösen eines CAPTCHAs benötigt). Lohnt es sich, als CAPTCHA-Löser zu arbeiten?

Aufgabe 5 (Firewalls). Sie haben in der Vorlesung Firewalls kennengelernt. Dabei handelt es sich um ein Sicherungssystem, welches Server und lokale Computer vor Zugriffen von außen schützt. Auf dem letzten Übungsblatt haben wir das Thema Firewalls schonmal kurz behandelt.

1. Erläutern Sie den Unterschied zwischen zustandslosen und zustandsbasierten Firewalls.

2. Im Folgenden sehen Sie Pakete, die sich Client und Server gegenseitig über zwei Firewalls senden (siehe Grafik). Außerdem sind zwei Arten von Firewalls eingerichtet:
Firewall 1 (zustandsbasiert): blockiert alle Anfragen, die häufiger als zweimal hintereinander vom gleichen Port und gleicher IP-Adresse ankommen, sowie Anfragen an Port 7263, wenn es zuvor eine Anfrage an Port 2837 gab.
Firewall 2 (zustandslos): Blockiert alle Anfragen von Port 2737 und an Port 7263.
Geben Sie für jedes Paket an, bei welcher Einstellung es durchgelassen wird und bei welcher es blockiert wird.



3. Wieso werden zusätzlich zu Firewalls auch noch Intrusion Detection Systeme (IDS) und Intrusion Prevention Systeme (IPS) benötigt?

4. Um DoS-Angriffe zu verhindern, legen Sie eine dynamische Regel in einer zustandsbasierten Firewall fest, die dafür sorgt, dass alle IP-Adressen gesperrt werden, von denen in kurzer Zeit viele Pakete geschickt werden. Wieso ist das keine gute Idee? Welche bessere Möglichkeit gäbe es?

Hausübung. Dieser Bereich ist dazu gedacht das Gelernte weiter zu vertiefen. Dazu werden je nach Themen weitere Übungsaufgaben, ergänzende Beweise oder ähnliche Aufgaben gestellt. Die Aufgaben sind freiwillig, können aber, bei erfolgreicher Bearbeitung, zu Bonuspunkten in der Klausur führen. Die Abgabe dieser Übungen erfolgt über **moodle** und kann in Gruppen mit bis zu vier Studenten (aus Ihrer **eigenen** Übungsgruppe) eingereicht werden. Abgaben werden nur als **.pdf-Dateien** akzeptiert. Denken Sie bitte daran, dass Ihre Lösungen nachvollziehbar und entsprechend ausführlich dargestellt werden sollen.

Für Gruppenabgaben ist folgendes zu beachten: Sie müssen in der Abgabe (.pdf-Datei) deutlich und eindeutig kennzeichnen mit welchen Gruppenpartnern die Aufgaben gelöst wurden.

Der Fachbereich Informatik misst der Einhaltung der Grundregeln der wissenschaftlichen Ethik großen Wert bei. Zu diesen gehört auch die strikte Verfolgung von Plagiarismus. Falls dieser Fall eintritt, behalten wir uns das Recht vor für diese Abgabe den jeweiligen Gruppen keine Punkte gutzuschreiben.

Bitte reichen Sie Ihre Abgabe bis **spätestens Freitag 01.02.2019 um 11:40 Uhr** ein. Verspätete Abgaben können **nicht** berücksichtigt werden.

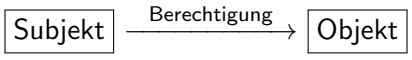
Hausübung 1 (Bell-LaPadula Modell (2 Punkte)). Wir betrachten ein vereinfachtes Modell der Zugriffsrechte einer Bank, in der ein Kassierer, ein Bankangestellter und ein Fachprüfer beschäftigt sind. Ferner sollen auch Kunden und das Finanzamt in den Zugriffsrechten berücksichtigt werden. In der Bank werden folgende Dokumente geführt:

1. Kundendaten (enthalten Name, Anschrift, Kundennummer etc., pro Kunde)
2. Kontodaten (enthalten Kontoinformationen pro Kunde, aber keine Transaktionen)
3. Transaktionshistorie (Übersicht pro Kunde)
4. Fachprüfungsbericht (enthält Details über sämtliche Kunden, deren Konten, sowie Transaktionen)

Der folgende Arbeitsablauf ist vorgesehen:

- Kundendaten dürfen NUR von Kunden geändert werden, aber Bankangestellte dürfen diese lesen
- Zum Schreiben des Fachprüfungsberichts braucht der Fachprüfer Lesezugruff auf die Kunden- und Kontendaten, sowie die Transaktionshistorie
- Der Kassierer ist in die Stufe *vertraulich* (2) einzuordnen.
- Der Fachprüfungsbericht darf NUR vom Fachprüfer gelesen werden.
- Das Finanzamt darf NUR Kunden- und Kontendaten lesen.
- Kontodaten dürfen vom Kassierer gelesen und geändert werden.
- Die Transaktionshistorie darf nicht vom Fachprüfer bearbeitet werden.

Aufgabe: Vergeben Sie an die oben angegebenen Rollen (Subjekte) Rechte, um die genannten Arbeitsschritte zu ermöglichen. Wichtig sind die Arbeitsschritte in denen ein "NUR" vorkommt. In diesen Fällen müssen Sie darauf achten, dass andere Rechte nach Definition des Bell-LaPadula Modells gar nicht vergeben werden dürfen. Tragen Sie diese Rechte in die untenstehende Tabelle ein, indem Sie den Subjekten und Objekten die Sicherheitsstufen *unklassifiziert*(1), *vertraulich*(2), *geheim*(3) und *streng geheim*(4) zuordnen, sodass jede Sicherheitsstufen mindestens ein Subjekt enthält. Verbinden Sie weiterhin die Subjekte mit den Objekten mit Pfeilen, die mit den entsprechenden Rechten versehen sind. Beispielsweise können Sie folgende Notation benutzen:



Verwenden Sie zur Lösung der Aufgabe eine Tabelle nach dem folgenden Muster:

Streng geheim
Geheim
Vertraulich
Unklassifiziert

Hausübung 2 (Authentisierungsprotokoll (1+2 Punkte)). Zwei Parteien A und B wollen sich gegenseitig authentifizieren. Bei der Authentisierung sollen folgende Bedingungen erfüllt sein:

- wechselseitige Authentisierung der beiden Parteien
- Authentisierung durch Wissen
- das Wissen darf beim Authentisierungsvorgang nicht übertragen werden
- auf einem asymmetrischen Kryptosystem basierend (z.B. RSA)
- sicher gegen Replay-Attacken

a) Sei nun folgendes Authentisierungsprotokoll gegeben: Die Parteien A und B besitzen jeweils ein asymmetrisches Schlüsselpaar (K_A^S, K_A^P) und (K_B^S, K_B^P) welche von einer Certification Authority (CA) generiert wurden. Weiterhin hat die CA jeweils ein zugehöriges Zertifikat Zert_A bzw. Zert_B erzeugt. Um sich zu authorisieren, schicken sich beide Parteien das jeweilige Zertifikat zu:

$$\underline{\text{A}} \qquad\qquad \underline{\text{B}}$$
$$\xrightarrow{\quad \text{Zert}_A \quad}$$
$$\xleftarrow{\quad \text{Zert}_B \quad}$$

Begründen Sie, dass das Protokoll mindestens eine der oben genannten Bedingungen nicht erfüllt.

b) Entwickeln Sie ein geeignetes Protokoll, das die geforderten Eigenschaften erfüllt. Geben Sie dazu die einzelnen Protokollschritte Ihres Systems und alle benötigten Informationen an (Kenntnis von Schlüsseln, transferierte Daten und Berechnungen bzw. Überprüfungen)!
Hinweis: Es kann sich an Challenge-Response-Verfahren aus der VL orientiert werden.

Hausübung 3 (Biometrie $(1 + 1 + 1 + (1 + 1)$ Punkte)). Eine Behörde nutzt zur Zugangskontrolle an ihrem Eingang ein biometrisches Authentifikationssystem. Das biometrische Merkmal wird gemessen, es wird mit einem in der Datenbank hinterlegten Muster verglichen und es wird ein Ähnlichkeits-Score errechnet, anhand dem entschieden wird, ob die Person akzeptiert oder zurückgewiesen wird. Das System weist folgende Fehlerraten auf:

False Acceptance Rate (FAR) beträgt 0,290%
False Reject Rate (FRR) beträgt 2,417%

a) Beim täglichen Eintreten von 940 berechtigten und registrierten Personen werden vom biometrischen System im Schnitt wie viele Personen abgewiesen?

b) Was zeigt Ihnen die untenstehende Abbildung? Welche Bedeutung hat die horizontale Achse? Wobei kann diese Abbildung helfen, wenn ein biometrisches Authentifizierungssystem konfiguriert wird? Auf welchen Threshold (Schwellenwert) ist das System der Behörde eingestellt?

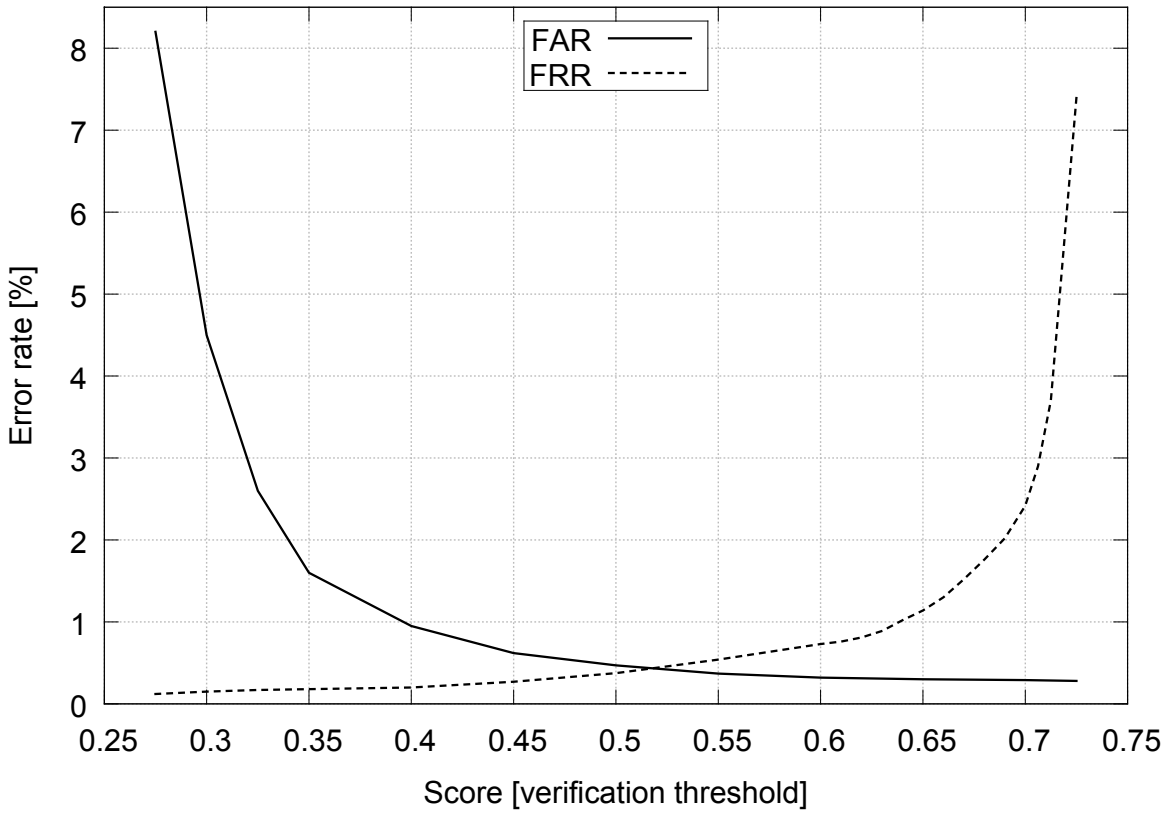
c) Als Kennwert für die Genauigkeit eines biometrischen Zugangskontrollsystems wird oft die so genannte Equal Error Rate (EER) angegeben. Die EER ist die Error Rate des Punktes, an dem FAR und FRR identisch sind.
Wo kann man diese in der untenstehenden Abbildung erkennen? Wie hoch ist ungefähr die EER und welche Aussagen über das System erlaubt diese?

d) Nehmen Sie nun – bei identischen Fehlerraten – an, dass von 10 der 940 Personen die Berechtigung revoziert wurde, diese aber weiterhin täglich versuchen einzutreten.
Wie hoch ist die Wahrscheinlichkeit, dass . . .

   i) ... eine Person, die Zutritt erhalten hat, unberechtigt ist?
   Hinweis: Nutzen Sie ggf. den Satz von Bayes.

   ii) ... eine Person, die nicht Zutritt erhalten hat, berechtigt ist?

Hinweis: Runden Sie auf fünf Nachkommastellen.



Hausübung 4 (Cipher Suites (1+1 Punkt)). Die Protokollsuite SSL/TLS ermöglicht dem Client, seine bevorzugten Cipher Suites selbst zu wählen. Nehmen wir an, folgende Cipher Suites stehen

zur Wahl, wobei die hier gegebene Reihenfolge auch die Reihenfolge ihrer Stärke ist und die Dritte als unsicher gilt:

- `ECDHE_RSA_WITH_AES_128_GCM_SHA256`
- `DHE_RSA_WITH_CHACHA20_POLY1305_SHA256`
- `RSA_WITH_RC4_128_MD5`

Nehmen wir weiter an, dass der Server alle möglichen SSL-Cipher Suites unterstützt (nicht nur die oben aufgeführten) und der Server wählt immer die Stärkste aus der Liste der Cipher Suites.

Ein sicherheitsbewusster Client, der seine Cipher Suite unabhängig von den Server-Einstellungen wählen kann, kontaktiert den Server in diesem Ablauf:

1. Der Client verbindet sich mit dem Server, indem er `ECDHE_RSA_WITH_AES_128_GCM_SHA256` als mögliche Cipher Suite angibt.
2. Wenn der Server dies ablehnen sollte, versucht der Client sich mit der nächsten Cipher Suite zu verbinden (`DHE_RSA_WITH_CHACHA20_POLY1305_SHA256`).
3. Dies wiederholt der Client für die nächste(n) Cipher Suites aus seiner Liste, bis der Server eine akzeptiert.

a) Begründen Sie, wieso dieser Ablauf für eine sichere Kommunikation genügt oder geben Sie ein Angriffsbeispiel an.

b) Worauf muss der Client achten, damit kein Man-in-the-Middle-Angriff (z.B. Cipher-Suite-Downgrade Attack) möglich ist? Geben Sie einen Ablauf der Auswahl der Cipher Suites zwischen Client/Server an und begründen Sie, wieso diese Lösung vor einem MitM-Angriff schützt.