Klausuranteil / Exam part
Einführung in die IT-Sicherheit / Introduction to IT Security

Prof. Dr. Hanno Langweg

2022-07-22T1200 – 2022-07-22T1330

- 6 Blätter inkl. Deckblatt / *6 pages including this front page*
- Bearbeitungsdauer: **ca. 45 Minuten (90 Minuten für gesamte Modulprüfung 6 ECTS)**
  *Available time **ca. 45 minutes (90 minutes for complete exam 6 ECTS)***
- Zugelassene Hilfsmittel: keine
  No permitted examination aids
- Schreiben Sie Ihren Namen und Ihre Matrikelnummer auf **jede** Seite
  *Write your name and student number on **each** page*
- Benutzen Sie nur das Klausurpapier (Rückseite, wenn nötig)
  Use only paper handed out (use reverse side of page if necessary)
- Schreiben Sie **lesbar**. Verwenden Sie einen schwarzen oder blauen Stift, keinen roten oder grünen.
  Write legibly. Use a black or a blue pen, do not use a red or a green one.

Congratulations - you successfully guessed the correct password!

This is the exam of the previous semester. Sorry, the current exam will not be released in advance ...

Vorname: _____ Nachname: _____
Given name *Family name*

Matrikelnr.: _____ ☐ AIN ☐ WIN ☐ Anderer Studiengang
Student number *Study programme* *(other)*

Regelmäßige Teilnahme an der Lehrveranstaltung in diesem Semester: ☐ ja ☐ nein
I attended classes regularly during the semester: *yes* *no*

Allen, die gelernt haben, wünsche ich viel Erfolg und allen anderen viel Glück!

Good luck!

1. **IT-Grundschutz / IT Base Protection (6%)**
2. **Ransomware (8%)**
3. **Zugriffssteuerung / Access Control (4%+3%+4%=11%)**
4. **Positivlisten / Whitelisting (8%+2%+6%+4%=20%)**

Name: _____ Matrikelnr.: _____

1. IT-Grundschutz / IT Base Protection (6%)

Kreuzen Sie alle richtigen und nur die richtigen Antworten an.
Mark all correct answers and only correct answers.

Was müssen Sie prüfen, wenn Sie die Umsetzung von Sicherheitsmaßnahmen planen?
What do you need to check when planning the implementation of security controls?

O Welche begleitenden Maßnahmen für eine erfolgreiche Umsetzung erforderlich sind
Which accompanying measure are necessary for a successful implementation

O Ob die betreffende Maßnahme bereits eingeführt ist
If the control has been implemented already

O Ob die Maßnahme mit anderen Maßnahmen vereinbar ist
If the control is compatible with other controls

O In welcher Reihenfolge die verschiedenen Maßnahmen umgesetzt werden sollen
In what order the various controls should be implemented

Was unternehmen Sie als Informationssicherheitsbeauftragter, wenn die Leitung Ihrer Institution nicht bereit ist, den Aufwand für eine bestimmte Sicherheitsmaßnahme zu tragen?
What do you do as Information Security Officer when the management of your organisation is not willing to bear the effort for a specific security control?

O Sie verdeutlichen ihr, welche Risiken mit dem Fehlen der Maßnahme verbunden sind.
You make clear what risks are associated with the missing security control

O Sie bitten die Leitung, durch Unterschrift zu bestätigen, dass sie die damit verbundenen Gefahren kennt und trägt.
You ask management for written confirmation that it is aware of the risk and is willing to take it.

O Sie ignorieren die Leitung und setzen die Maßnahme trotzdem um.
You ignore management and implement the controls anyway.

O Sie verzichten auf eine unmittelbare Reaktion, nehmen sich aber vor, nach Ablauf einer gewissen *Zeitspanne* die Zustimmung der Leitung einzuholen.
You do not react immediately, but you plan for getting management support after a certain time has passed.

Wer sollte in der Regel technische Maßnahmen zur Absicherung eines bestimmten IT-Systems umsetzen?
Who should usually implement technical controls to secure a specific IT system?

O Die Leitung der IT-Abteilung
The head of the IT department

O Der Informationssicherheitsbeauftragte
The information Security Officer

O Der zuständige Systemadministrator
The responsible system administrator

O Der Benutzer des IT-Systems
The user of the IT system

Name: _____ Matrikelnr.: _____

2. Ransomware (8%)

Bei einem sogenannten Ransomware-Angriff (Ransom engl. Lösegeld, Ransomware = Ransom+Malware) verschaffen sich Angreifer Zugang zum Gerät eines Betroffenen und verschlüsseln Daten auf dem Gerät. Anschließend verlangen die Angreifer Geld im Austausch gegen das Versprechen der Entschlüsselung.
*In a ransomware attack (**ransom**+mal**ware**), attackers – after obtaining access to a victim's machine – encrypt a victim's data and request money in exchange for decrypting the data.*

Zwei übliche Angriffsvektoren für Ransomware sind die Ausführung von Schadsoftware oder das Ausnutzen einer Softwareschwachstelle in einem Netzwerkdienst. Nennen Sie für diese beiden Angriffsvektoren je ein geeignetes Entwurfsprinzip von Saltzer und Schroeder, gegen das verstoßen wird, um den Angriff zu ermöglichen. Nennen Sie für jeden der beiden Angriffsvektoren eine geeignete Schutzmaßnahme.
Two typical attack vectors for ransomware are execution of malware or exploitation of a software vulnerability in a network service. Name for each of the two attack vectors a suitable design principle of Saltzer and Schroeder that is violated to enable the attack. Name for each of the two attack vectors an appropriate protection mechanism.

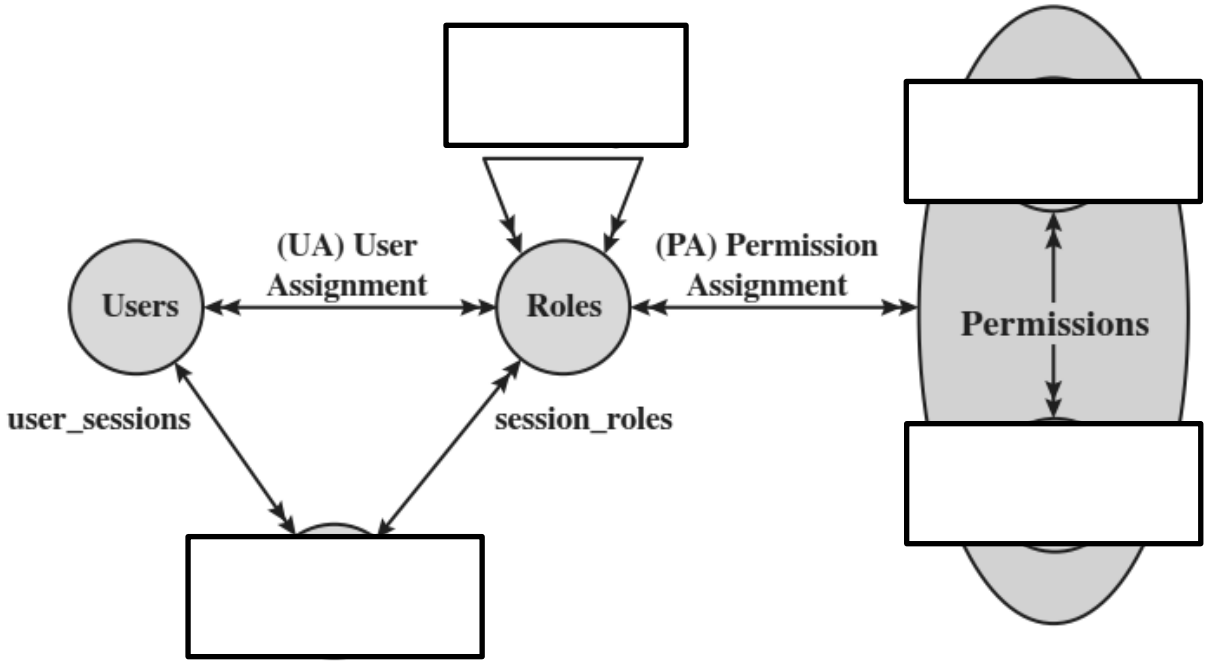
3. Zugriffssteuerung / Access Control (4%+3%+4%=11%)

Was ist der Unterschied zwischen einer NULL DACL und einer leeren DACL?
What is the difference between a NULL DACL and an empty DACL?

Name: _____ Matrikelnr.: _____

Was ist der Unterschied zwischen einem (systemweiten) Privileg und der Zugriffsmaske in einem Zugriffssteuerungslisteneintrag (ACE)? Und: Geben Sie ein Beispiel für ein Privileg in Windows.
What is the difference between a system-wide privilege and an access mask in an ACE? And: Give an example for a privilege in Windows.

Komplettieren Sie das nachfolgende Diagramm bezüglich RBAC Role Based Access Control.
Complete the diagram with respect to role-based access control (RBAC).



Stallings/Brown (2015). Computer Security. Fig. 4.8

Name: _____ Matrikelnr.: _____

4. Positivlisten / Whitelisting (8%+2%+6%+4%=20%)

Positivlisten für Anwendungsprogramme regeln, dass nur solche Anwendungsprogramme ausgeführt werden können, die von der Organisation für ein Benutzerkonto oder für ein Gerät zugelassen worden sind. Für Microsoft Windows werden Positivlisten beispielsweise mittels AppLocker und Windows Defender Application Control (WDAC) umgesetzt.
Whitelists for applications can be used to enforce that only those applications can be executed that are specifically allowed by an organisation for a user account or for a device. For Microsoft Windows, application whitelists can be managed using, e.g., AppLocker and Windows Defender Application Control (WDAC).

a) Beschreiben Sie die Funktionsweise von AppLocker oder WDAC.
Describe how AppLocker or WDAC works.

b) Wozu dient der Audit Mode?
What is the purpose of the audit mode?

c) Welchen konkreten Inhalt empfehlen Sie für eine pfadbasierte Positivliste (Whitelist) für einen Arbeitsplatz-PC in der Verwaltung einer Hochschule? Antworten Sie, ohne die im einzelnen benötigten Anwendungsprogramme zu kennen. Das Ziel ist, dass die Ausführung von Schadsoftware verhindert wird.
What specific content of a path-based whitelist do you recommend for a personal computer of the administrative department of a university? Answer without knowing the particular applications that are used. The goal is to prevent the execution of malware.

d) Welche Herausforderungen sehen Sie für Positivlisten in PC-Pools einer Hochschule? Welche zusätzlichen oder alternativen Schutzmechanismen empfehlen Sie bei einer geplanten Einführung von Positivlisten für PC-Pools?
What challenges do you see for whitelists for computer labs at a university? What additional or alternative protection mechanisms do you recommend for a planned introduction of whitelists for computer labs?