# Musteraufgaben

Aufgabe1: Einzel Erklärung der Worte

Beschreiben sie den Zusammenhang der begriffe Bedrohung Angriff Schwachstelle Risiko.

Lösung: Hab nur ein Risiko wenn es eine Bedrohung und eine Schwachstelle gibt auf die die Bedrohung Zielt.

Angriff ist die Umsetzung dieser Bedrohung (Bild in Folie mit Pfeilen).

Aufgabe2: Widersprechende Sicherheitsziele

Bei der Umsetzung eines Sicherheitszieles können Situationen auftreten, die die Umsetzung zusätzlicher Sicherheitsziele (ggfs. für zusätzliche Informationsobjekte ) erfordern. Geben sie dafür ein Beispiel.

Lösung: Vertraulichkeit, Integrität Verfügbarkeit.

Schutzziel Vertraulichkeit-> Verschlüsselung Mechanismus-> Brauche Schlüssel -> Richtige Schlüssel->Schlüssel müssen Integritätsgeschützt sein. <- Neues Schutzziel Integrität

Aufgabe3:

Wir beziehen uns auf das Szenario eines Online-Kurses aus der Vorlesung (Einreichen von Hausaufgaben, Abholen einer Musterlösung)

a.) Welche Schutzziele würden sie als Betreiber einer solchen Lösung fordern

Lösung: Vertraulichkeit (keiner soll abschreiben können)

Integrität der Musterlösung und der Haushaufgaben.

Verfügbarkeit (Nicht das man kurz vor Abgabeende nicht abgeben kann)

Privacy (Datenschutz -> Keiner soll wissen ob ich schon abgegeben hab oder nicht)

...

b.) Geben sie die Maßnahmen für die Schutzziele an.

Lösung: Regeln müssen definiert und Kontrolliert werden.

Aufgabe4:

Erklären sie den Unterschied zwischen "Sicherheitspolitik" und "Sicherheitsmodell".

Lösung: Eigentlich wird es gleichermaßen genutzt

Sicherheitspolitik -> Textuelle Beschreibung

Sicherheitsmodell -> Ist eine Präzise Formale Beschreibung der Politik (irgendwleche Lustigen Formeln).

Aufgabe5: Vergleich anderer Sicherheitspolitiken

Welche Vorteile bietet eine rollenbasierte Sicherheitspolitik und Vergleich zu einer Identitätsbasierten Sicherheitspolitik.

Lösung: Auch

Vorteile rollenbasiert: Nutzer hat eine Rolle und darf a und b es gibt zum Beispiel 10 Rollen. Lesen der Zugriffsrechte deutlich übersichtlicher und schneller änderbar. Da man auf eine Gruppe von Nutzern zugreifen kann und nicht nur auf einzelne.

Vorteile Identitäsbasierten: Für jedes Sunjekt, Objekt müssen Regeln da sein. Wird sehr schnell sehr groß. Bei 100.000 Nutzern und 1000 Objekten -> Bei betrachten der Rechte über 100.000.000 Rechte

Aufgabe 6: Andere Modelle Vergleichen

Erklären sie in welcher Hinsicht das Modell der Lamportschen Zugriffsmatrix "schwächer" als das HRU-Modell ist. Verdeutlichen sie dies auch an einem Beispiel.

Lösung: Geht besseres Beispiel

Zugriffsmatrix ist statisch. Änderungen können nicht betrachtet werden(Rechte und Objektänderungen können nicht beschrieben werden).

Matrizen sind einzelne states die sich dynamisch mit den im HRU Modell beschriebenen Regeln ändern lassen.

Zwei Nutzer 2 Dateien. Wenn sich die Rechte der Nutzer auf die andere Datei verschieben kann diese Änderung nur im HRU-Modell beschrieben werden, nicht aber in der Lamportschen Zugriffsmatrix.

Aufgabe7:

Betrachten sie folgende Aussage "Zugriffssteuerungslisten sind mächtiger als Capability-Listen"

a.) Stimmt diese Aussage?

Lösung: Unterschiedliche Darstellung des Selben Inhalts. Diese Darstellung kann Vor und Nachteile haben.

b.) Welche Vor-/Nachteile haben diese Listenarten(jeweils)? Begründen Sie?

Lösung: Wenn ich nach den Zugriffsrechten auf ein bestimmtes Objekt suche und die Falsche Listendarstellung habe wird mein Aufwand immens erhöht.

c.)Welche Probleme ergeben sich bei der Umsetzung der Capability-Listen in verteilten Systemen.

Aufgabe8:

Sie sollen ein einfaches Zugriffssystem für eine verteilte Literaturdatenbank entwerfen. Grundsätzlich soll jeder zugelassene Nutzer Lese-und Schreibrechte auf alle Literatureinträge haben Es soll einen Administrator geben, der neue Nutzer anlegen und existierende Nutzer löschen kann. Der Administrator selbst ist kein Nutzer und darf die Literatureinträge weder lesen noch schreiben.

a.) Welche Art von Sicherheitspolitik schlagen Sie vor?( Wählen Sie eine möglichst einfache Lösung). Begründen sie ihre Entscheidung.

Lösung:

Wir beschrieben Verbal unsere Politik. Jeder zugelassene(gibt auch nicht zugelassene) Nutzer kann Lese und schreibrechte auf alle Literatureinträge.

Admin darf neue Nutzer anlegen und existierende Nutzer löschen.

Admin ist kein zugelassener Nutzer (darf nicht lesen und schreiben)

-> Lampartsche Zugriffsmatrix scheitert -> Admin baut neue Nutzer und damit neue Zugriffe ein.

->HRU-Modell funktioniert da es die Änderungen der vom Admin ausgehenden Aktionen umsetzen kann.

b.)Ist die Safety von Zuständen in der von Ihnen vorgeschlagenen Lösung entscheidbar?

Lösung:

HRU-Modell hat generell keine entscheidbaren Zustände. Alle Nutzer hat alle Rechte (Admin selbst ist kein Nutzer also bekommt er keine neuen Rechte). Wir haben also einen Zustand und ein Recht und können Logisch entscheiden das HRU-Modell in diesem Fall entscheidbar ist.