

Sicherheit: Fragen und Lösungsansätze – Übung 6

AUFGABE 1(Chinese-Wall) (4BP):

Weil Eva sich ausgeschlossen fühlt, hat sie Peter dazu überredet, das Zugriffssystem zu einem Chinese-Wall-Modell zu ändern. Dabei existieren nun für den Bereich oder die Konfliktklasse Zeitplaner die “Unternehmen” oder eher Teilbereiche {Hauptfachvorlesungen, Nebenfachvorlesungen, zusätzliche Interessen, Hochschulsport}, für den Bereich Finanzen die Teilbereiche {BaFöG, Nebenjob, Zuschüsse der Familie} und für den Bereich Freizeit die Teilbereiche {UFC, AGs, Sportverein, Party}. Die fertigen Dateien seien öffentlich.

Skizzieren Sie das Chinese-Wall-Modell einmal initial, und einmal nach jedem Zugriff aus Sicht des gerade Zugreifenden. Nehmen Sie dazu an, dass in jedem Teilbereich nur ein Objekt existiert, und alle Zugriff Lesezugriff sind.

1. Alice greift auf Hochschulsport zu.
2. Bob greift auf BaFöG zu.
3. Peter greift auf AGs zu.
4. Eva greift auf Hauptfachvorlesungen zu.
5. Bob greift auf zusätzliche Interessen zu.
6. Bob greift auf UFC zu.
7. Peter greift auf UFC zu.

Eva hat einen Fehler in die Verwaltung des Chinese-Wall-Modells eingeschmuggelt: Die Zugriffshistorie wird nur für die letzten beiden von diesem Nutzer besuchten Bereiche festgehalten, besucht er einen Weiteren, wird die Historie des ältesten Bereichs gelöscht.

Kann Eva alle Teilbereiche einsehen, ohne einen zweimal zu Besuchen? Notieren Sie den dazu nötigen Pfad.

Was wäre geschehen, hätte Bob in 5. statt Lesezugriff einen Schreibzugriff verlangt?

AUFGABE 2(Isolation) (2LP):

Beschreiben Sie kurz (max 200 Wörter), wieso die Isolation für Zugriffssysteme existentiell ist.

AUFGABE 3(IPSec) (4LP):

Im folgenden sei Ihnen ein IP-Paket schematisch angegeben.

Erstellen Sie darauf basieren das Schema eines IPSec-Paketes, im AH-Tunnel-Mode. Verwenden Sie zur Bildung der “Integrity Check Value” 256-AES-RSA-MD5, und beschriften Sie das passende Feld entsprechend.

Markieren Sie in Ihrem Schema, welche Felder sich besonders von denen des originalen IP-Paketes unterscheiden, und wo in dem neuen Paket das Original “untergebracht” ist. Beschreiben Sie Ihre Vorgehensweise ausführlich.

ver	hlen	TOS	pkt len	
ID			flgs	frag offset
TTL	proto=TCP		header cksum	
scr IP address				
dest IP address				
TCP header (proto = 6)				
TCP payload				