Information Security, 2015–2016

Prof.Dr. Ferucio Laurenţiu Ţiplea
Department of Computer Science
"Al.I.Cuza" University of Iaşi
Office: C 301
Tel: (0232) 201538

Date: Jan 22, 2016

Examen (timp de lucru: 1h40')

1. (Politici de securitate – timp estimat: 40')

   (a) Descrieţi modelul Bell-LaPadula (explicaţi clar fiecare notaţie utilizată). **0.75p**

   (b) Descrieţi modelul Biba (explicaţi clar fiecare notaţie utilizată). **0.75p**

   (c) In Figura 1 aveţi două latici de clase de securitate. Utilizaţi una dintre ele pentru a ilustra modelul Bell-LaPadula, iar cealaltă pentru modelul Biba.

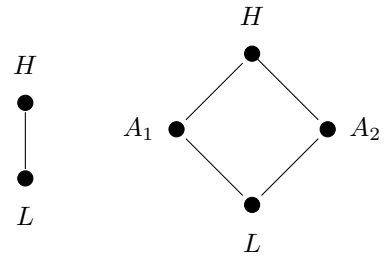

Figure 1: Latici de securitate

0.5p

   (d) Combinaţi modelele de la punctul anterior intr-un singur model şi explicaţi-l. **2p**

2. (IPsec – timp estimat 30') Presupunem că ESP în modul transport încapsulează segmente TCP, iar aceste segmente sunt criptate în modul CBC. Dacă un intrus are acces (citire şi modificare) la vectorul de iniţializare IV al modului de criptare, poate acesta monta un atac cu succes? Discutaţi toate variantele posibile ce credeţi că pot conduce la atac, şi argumentaţi-le cât mai riguros. **3p**

   Notă: Structura unui segment TCP este cea de mai jos:

16-bit sourrce port number								16-bit destination port number
32-bit sequence number								
32-bit acknowledgment number								
header length	reserved	URG	ACK	PSH	RST	SYN	FIN	16-bit window size
16-bit TCP checksum								16-bit urgent pointer
options (if any)								
data bytes (if any)								

Figure 2: Format segment TCP

Soluţie: (schiţă) Primii 64 bits ai headerului TCP conţin adresa destinaţie. Dacă intrusul are acces la IV (citire/modificare), atunci el poate modifica IV astfel încât să se rescrie adresa destinaţie printr-o adresă pe care el o poate controla (în modul CBC, primul pas este de a cripta XOR-ul dintre IV şi primul bloc de mesaj care este măcar de 64 bits). O astfel de modificare nu afectează modul de criptare/decriptare

şi nici rezultatul decriptării, exceptând faptul că adresa destinaţie va fi cea dată de intrus. In acest fel, intrusul obţine mesajul original.

Şi modificări ale câmpurilor ce conţin numărul de secvenţă sau dimensiunea ferestrei pot cauza anomalii (chiar dacă acestea nu sunt la fel de puternice ca atacul de mai sus).

3. (Controlul accesului – timp estimat 30') Arătaţi că pentru orice graf orientat finit $G = (V, E)$ se poate construi, în timp polinomial în raport cu dimensiunea grafului, un sistem de protecţie mono-operaţional peste o mulţime R de drepturi, o stare Q a acestuia şi se poate specifica un drept $r \in R$ astfel încât G admite o clică de dimensiune k ($k \leq |V|$) dacă şi numai dacă Q nu este sigură pentru r. **3p**

Soluţie: (schiţă) The clique problem is the problem to decide, given an undirected graph $G = (V, E)$ and an integer k, whether G has a clique of dimension k (also called a k-clique). A k-clique in G is a subgraph of G with k nodes and wherein every two distinct nodes are connected by an edge.

Given $G = (V, E)$ and k an instance of the clique problem, consider a set $R = \{edge, leak\}$ of rights and define the state $Q = (V, V, A)$, where

$$A(x, y) = \begin{cases} \{edge\}, & \text{if } (x, y) \in E \text{ and } x \neq y \\ \emptyset, & \text{otherwise} \end{cases}$$

for all $x, y \in V$.

Consider now the mono-operational protection system $\mathcal{C}$ consisting of exactly one command

$$Clique(X_1, \ldots, X_k)$$

given by

command $Clique(X_1, \ldots, X_k)$
  if
    edge in (X_i, X_j) $\forall i, j \in \{1, \ldots, k\}$ with $i \neq j$
  then
    enter leak into (X_1, X_1)
end

(the "$\forall \ldots$" part in this command is a shortcut for the conjunction of all membership tests indexed by i and j).

It is straightforward to prove that G has a k-clique if and only if Q is unsafe for *leak* w.r.t. $\mathcal{C}$.