Information Security, 2014–2015

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

Date: Jan 29, 2014

Examen Final (timp de lucru: 1h40')

1. (IPsec – timp estimat: 30')
   (a) Ce este o asociere de securitate în IPsec şi care sunt mecanismele de securitate fundamentale din IPsec? **1p**
   (b) Descrieţi, succint dar clar, protocolul AH în cele două moduri de utilizare pentru datagrame IPv4. **1p**
   (c) Descrieţi, succint dar clar, protocolul ESP în cele două moduri de utilizare pentru datagrame IPv4. **1p**
   (d) Descrieţi câteva combinaţii de asocieri de securitate in IPsec (end-to-end, VPN, end-to-end cu VPN). **1p**

2. (DNSsec – timp estimat: 40')
   (a) Descrieţi, succint dar clar, modul de funcţionare a protocolului DNS. **1.5p**
   (b) Descrieţi, succint dar clar, modul de funcţionare a protocolului $DNSsec$. **1.5p**
   (c) Prezentaţi şi discutaţi 2 argumente pentru care credeţi că $DNSsec$ asigură securitate. **1p**

3. 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. **2p**

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

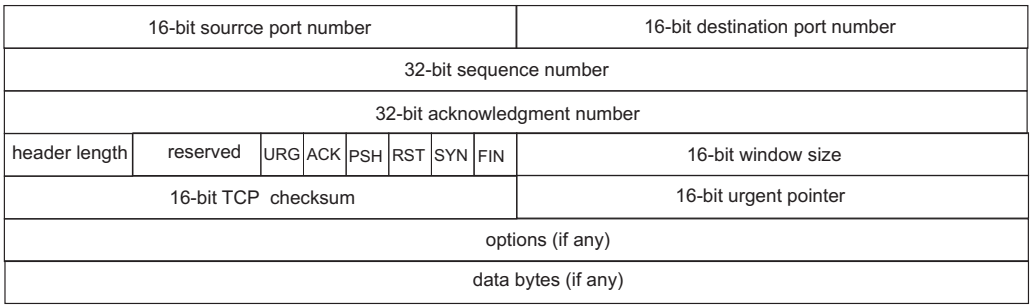

Figure 1: Format segment TCP