S-38.153 Security of Communication Protocols

Exam May 10. 2002/ J. Jormakka. Try to answer to every question, they are not impossible and a reasonable answer gives some points.

1 Spell out and explain briefly (one-two lines is enough) the following abbreviations:

a) C^3ISW
b) ECC
c) IPsec SPI
d) AAAARCH
e) CBC mode
f) IKE

2 Explain security of CGI. That is, explain briefly what is CGI and what are its vulnerabilities and describe some ways to solve the vulnerabilities.

3 How can a terrorist use the Internet for his purposes? Describe some attack types a cyber terrorist might utilize. How can a defender tell the difference between "harmless" hackers and terrorists, or can he?

4 How can a hacker gain information of the network or network element he wants to attack? What tools he can use? What information he tries to find? How can a defender hinder or make more difficult this collecting of information?

5 In eCommerce and mCommerce users should be able to buy products through the Internet, usually through a WWW interface (HTTP and WAP for mobiles). Most eCommerce systems use SSL, some use SET for credit card purchases. Design a possible eCommerce/ mCommerce solution by drawing an architecture, which explains what protocols, servers etc. you intend to use. Describe how users are authenticated in your solution, how privacy is provided if you need privacy in your solution, and how sufficient availability is made? Describe to what kind of purchases your solution suits. What vulnerabilities your solution has?