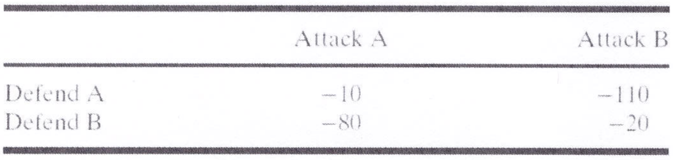
Cyber Risk Management mid-term exam, 6 October 2016, 15:45-17:45

TUDelft: SPM5440 (4EC), SPM5442 (5EC) UTwente: 201500026 (5EC)

Start each numbered question (1-5) on a new page. Min. 1 paragraph / max. 1 page per numbered question. Make sure that what you write is relevant to the question.

1. Give an argument (a) for and (b) against the proposition that security requirements (or policies) are derived from attack scenarios. Use the term asset in your answer. (10 pts)

2. In the paper by Cox Jr ("Game theory and risk analysis"), you can find the following table:

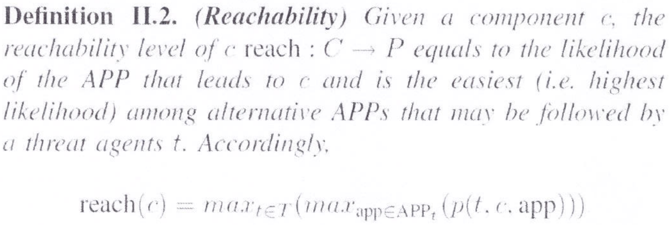


	Attack A	Attack B
Defend A	−10	−110
Defend B	−80	−20

   a. Explain what this table represents, and from which inputs the values in the table have been derived (there are 4 input numbers). (5 pts)

   b. Explain what you can calculate from tables like these, assuming simultaneous choices. Give both the term and the meaning. Explain the notion of "mixed-strategy" that is used in this context. (5 pts)

3. The following figure shows the definition of reachability in CRAC. (APP is Attack Propagation Path.)



Definition II.2. ***(Reachability)*** *Given a component c, the reachability level of c* reach : $C \rightarrow P$ *equals to the likelihood of the APP that leads to c and is the easiest (i.e. highest likelihood) among alternative APPs that may be followed by a threat agents t. Accordingly,*

$$\mathrm{reach}(c) = max_{t \in T}(max_{\mathrm{app} \in \mathrm{APP}_t}(p(t, c, \mathrm{app})))$$

Explain the relation between the weakest link concept and the notion of reachability in CRAC. Use the terms threat, vulnerability and impact in your answer. (10 pts)

4. There are said to be 4 options for risk treatment: accept, reduce, transfer and avoid. A company expects 5 incidents each year, with an impact of EUR 10,000 each. They can buy equipment for EUR 40,000 that they believe will prevent 3 out of 5 of those for at least 3 years. Alternatively, they can buy full insurance against those incidents for EUR 15,000 per year.

   a. For each of the 4 general risk treatment options, explain how they would influence the FAIR risk factors. (4 pts)

   b. Calculate the 3-year return on security investment (ROSI) of the equipment. (4 pts)

   c. What would be your recommendation to the company and why? (2 pts)

5. The term "critical" often shows up in cyber risk management, referring to potentially high impact.

   a. Give the three critical Internet resources Laura DeNardis describes in her article and describe why they are considered to be critical. (3 pts)

   b. Explain the relation between critical infrastructures, critical information infrastructures, and critical Internet resources. (3 pts)

   c. Describe a potentially controversial security control in critical infrastructures, and its relation to one of the debates discussed in the lecture on cyber governance. (4 pts)