2007 Paper 7 Question 15

Additional Topics

A large ski resort is organised as a consortium of hundreds of independently-owned lifts, each serving one or more ski slopes. The resort sells a non-transferable, photo-id based "skipass" ticket that lets its owner ride on a specified subset of the lifts, for a specified range of dates, for an unlimited number of rides. Each ticket has a different barcode and is scanned at the entry gate of each lift to decide whether to let the skier through.

The whole resort is about to upgrade from barcode to passive RFID: tickets with embedded RFID tags can be read through the pocket of the skier from a distance of about 5 cm. You have been hired as a security consultant by the resort to oversee the planned changeover.

(a) The operators have requested offline operation: like its barcode-based predecessor, the new system must permit the verification of tickets without requiring individual lifts to have a live connection to the central server all day long (or at all). Justify this request, then design a suitable system architecture and discuss the security implications of this requirement. [6 marks]

(b) Discuss as many ways as possible in which the consortium might be defrauded and suggest appropriate countermeasures. Label each fraud as "made easier by RFID" or "made harder by RFID". Your employers are slightly less interested in frauds that carry over unchanged between barcode and RFID: so, do mention them if you wish but don't over-analyse them. [8 marks]

(c) Small but vocal consumer groups complained about loss of privacy as soon as they heard that the system used RFID. Highlight any privacy threats introduced by RFID in this system. Design an alternative RFID-based architecture offering strong privacy protection for customers. Compare it, from any relevant viewpoints, against the legacy barcode system and against the privacy-indifferent RFID system you designed in part (a). [6 marks]