Lecture 27 Case Study
1.264, Fall 2013

A hotel uses magnetic stripe cards as room keys. The magnetic stripe card holds a maximum of 50 bytes (characters) of data. There is a server used by front desk staff that can write information to the magnetic stripe card when a guest checks in. The hotel room doors have a simple battery-powered device that can read the card. The hotel room door unit:

- Cannot write to the card
- Can store what it has read from cards in the past, up to 100 characters (bytes)
- Has a very simple clock that can only count days, up to 30 days
- Has no network communications
- Interacts only with the card; it can only read the card—it cannot write to the card
- Can open the physical lock on the door

a. Describe the security protocol that you would use between the magnetic stripe card and door unit. The server has a peripheral device that writes the data to the card; you don't need to consider the server as part of the protocol. The server can write the data your desire to the card.

You must, of course, consider the situation that a room is potentially rented to a different person every evening. You may assume that each customer checks out and returns the card at checkout. Use the protocol notation from lecture and the Anderson book.

b. Describe attacks on your proposed solution, and give examples under which they succeed or are successfully defended against, for the following:

1. A customer makes a copy of the card and sells it to someone.
2. Cut and paste attack
3. Replay attack

c. Discuss the role of encryption in this system. If your proposed protocol uses encryption, describe at least one attack that the encryption guards against. If your proposed protocol does not use encryption, briefly describe why.

1.264J / ESD.264J Database, Internet, and Systems Integration Technologies
Fall 2013