Lecture 27 Case Study Solution
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 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**
- **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. 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.

The mag stripe card must have a code (number) that unlocks the door. It must also have the previous code, and perhaps more than one previous code. We assume each code is 20 bytes. It also uses one byte to write the number of days that the room has been reserved. The server at the front desk writes these codes to the card.

When the guest inserts the card in the door unit, it reads the previous code(s); at least one of them must match previous codes used for that door. The door unit stores the previous code(s); this is the only way it has to determine if a new code should be accepted. The card with the new code must have one or more previous codes.

If the card has a previous code, the new code is written along with the number of days. The door unit will accept the current magnetic card with the new code for the number of days indicated on the card.

No reasonable cryptography is possible with a magnetic stripe card and a door unit with a minimal clock.

Call the card C and the door unit D:

C->D : N1, N2, N3, N4, T where N1 is the current code, N2, N3 and N4 are previous codes and T is the number of days the room is reserved

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

1. A copied card can be used. There is no protection in this protocol.
2. An attacker could rent a room for just one night and change the value of T to be several nights, allowing access on future nights if the room is vacant. However, if another guest reserves and uses the room, this protocol will invalidate the attacker's mag stripe card, since its code is now a 'previous' code.
3. Replay attacks are possible. A black hat could intercept the card-door interaction, write it to a new card, and enter the room. Mag stripe readers emit radiation that can be intercepted.

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.

This is a very weak protocol because of the limitations of the card and door unit and nothing will really make it stronger.
a. You could encrypt the data on the card but it could still be copied and vulnerable to a replay attack or a copied card. The attacker would not need to decrypt it. It would make it harder to do the cut and paste attack.
b. You can never tell the difference between the original card and a copied card. The original card is used repeatedly to open the door, so it must be good for multiple uses.