5 Software and Security Engineering (rja14)

The basic Europay-MasterCard-VISA transaction flow is

\[
\begin{align*}
C & \rightarrow T : \ PAN, d_1, \text{Cert}_{KB}(PAN, d_1) \\
T & \rightarrow C : \ N, t, X, d_2, \text{PIN} \\
C & \rightarrow T : \ d_3, \text{MAC}_{KCB}(d_3, T, N, t, X)
\end{align*}
\]

where \( C \) is the customer card, \( T \) the merchant terminal, \( d_1 \) the card data, \( PAN \) the primary account number, \( N \) the unpredictable number, \( t \) the date, \( X \) the amount, \( d_2 \) and \( d_3 \) the merchant data, \( KB \) the bank signing key, \( KCB \) the key shared between the bank and the card and \( \text{PIN} \) the customer PIN.

(a) How does the merchant terminal obtain authorisation from the card-issuing bank? \([4 \text{ marks}]\)

(b) Describe two attacks on this protocol that can be used to commit fraud. In each case describe the protocol flaw or system limitation responsible. \([8 \text{ marks}]\)

(c) You are a security engineer working for a payment network owned by a country’s banks. Which of the two attacks would most worry you, and what would you do to forestall or mitigate it? \([8 \text{ marks}]\)