COURSE: COMPUTER SECURITY AND PRIVACY CS6362
NAME: ELUWA CHIDERA DUANNE ANITA

CASE STUDY: SECURITY PROBLEMS FOR ATM SYSTEMS

This case study summarizes the security vulnerabilities in an ATM (Automated Teller Machine) usage that was described by an independent auditor named Redspin, Inc.

To successfully use an atm, it must consist of a) the user; the person whose card is being used and whose account is being debited. b) the issuer; the institution or organization that authorizes all transactions and debits to the user's card. c) the processor; the organization that provides core data processing to the issuers.

Over the years, the configuration of the ATM has rapidly changed and improved. In the early years of 2003, the atm units were linked to the processor and not the issuer who owned the machine itself. The typical illustration of how the atm was being used then is as follows; a user will swipe his card on the machine and enter a PIN (Personal Identification Number). The ATM will then encrypt the PIN using DES (Data Encryption Standard) and sends it to the processor after which the processor will update the user's information and sends a reply. However, by 2006 a higher encryption standard called Triple DES and the use of a protocol named TCP/IP for network transporting was introduced.
There was also an upgrade in the ATM's OS (Operating system).

After these were introduced, the ATM configuration changed. The units were no longer linked to the processors directly. Rather, the information sent from the ATM travels through the issuer's network first before getting to the processor. Now, this is where the vulnerability of the customer's information sets in.

As mentioned earlier, there was an upgrade in the ATM's OS and the encryption method from DES to Triple DES. However, these were the only information of the user or customer that was protected. Every other information such as the card details, account balance of the user, the withdrawal amount and many other information was not protected and were open to hackers and available for modification. This means that if a hacker gets access to the bank's network, he will have access to all the user's information mentioned above and much more. Thus, leading to the compromise of the Confidentiality and Integrity of the user's data or information.

Confidentiality as we all know is the protection of data from unauthorized users. But in this case, the customer's card details, account balances, and so on is exposed and any hacker can clone the card or use the details to perform fraudulent and unauthorized transactions online. This could also lead to the modification of the user's data or altering the data in transit. This is where the Integrity is tested.
The account balance could even be changed without the user ever knowing how it happened. Redspin however recommended two measures that banks could use to counter or mitigate these vulnerabilities and threats. One of the measures is a short-term fix. This includes segmenting ATM traffic from the networks by implementing a strict firewall rule or dividing the networks. Also, a network-level encryption can be implemented between routers where the ATM traffic travels. The second measure is the long-term fix where the application-level software is completely changed in order to protect the confidentiality and Integrity of the user's information. This includes encrypting all the customer's information that travels through the network and not just the PIN. Also, implementing a machine-machine authentication between the ATM and the processor and using challenge-response protocols to stop replay attacks. Hence, protecting the Integrity of data.