MOBILE CLIENT DEVICES AND PERVASIVE COMPUTING

Lesson 03

Smart Systems─ Cards, Labels, and tokens

1

Smart systems

- Have computational devices embedded into it
- Provide comfort, efficiency, and remote access to devices and appliances
- Smart cards, labels, tokens

Smart systems

- Widely used throughout the consumer goods and service industries

Smart Cards

- Smart cards multiple applications
- Numerous forms
- Credit cards
- Identification cards
- Key card for automobile, bike, home

Smart Cards

- Simple ones: memory cards, meant for storing data
- Rewriteable memory devices for storing and updating data

Smart Card Application development

- JavaCard language for application development

6

Smart Cards

- Contact smart cards
- ISO/IEC 7816 and ISO/IEC 7810 standards for size, shape, electrical characteristics, communications protocols and command formats

7

Contactless smartcards

- Contact-less cards communicate with the card readers using the RF (radio frequency) (Section 2.5.2) induction technology.

- Standard for contact-less smart card communications is ISO/IEC 14443

8

Smart cards

- Card— a secured hardware and circuit including a computer, memory, and transceiver

- Chip lies in-between the inner layers of the card

- A transceiver —a circuit for transmitting and receiving signals

Smart cards

- Do not have batteries
- Energy provided by the card reader
- The computer in the card activated by power
- Through radiation in a contact-less card

Smart cards applications

- For financial transactions as a credit card or ATM/debit card

- Store personal ID (even photo) and personal information

- Store the medical records of the holder

11

Smart cards applications

- An employee card in an enterprise to open the security locks at work and log in.

- A student card to get books issued from the college library

CARD COMMUNICATION WITH THE HOST

- Appropriate interchanges for authentication before communication ASK 13.56 Mbps used for contact-less communication at data rates of ~1 Mbps
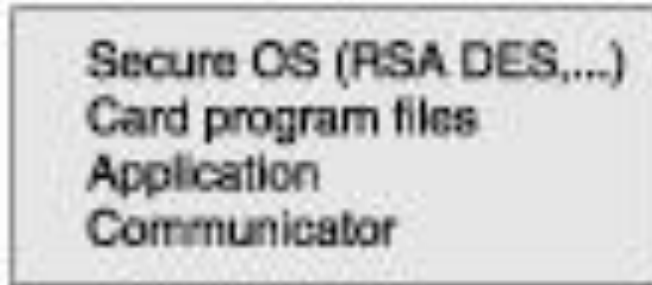- A metallic squared foil antenna

Card communication with the host

- The host— a device which reads the card and performs requested transactions
- The host connects to a PC or remote server through a phone line, Internet leased line, or a fibre line
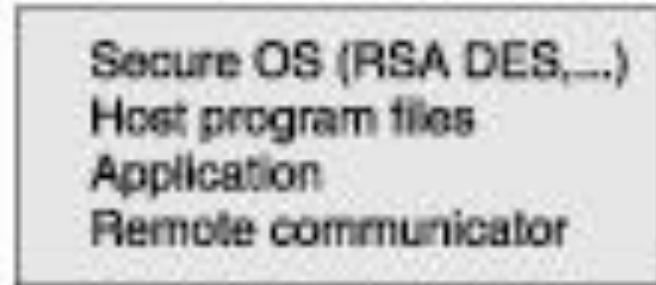
14

Smart card and its host

15

SOFTWARE COMPONENTS IN A SMART CARD

| Secure OS (RSA DES,...) |
| Card program files |
| Application |
| Communicator |

Card software

| Secure OS (RSA DES,...) |
| Host program files |
| Application |
| Remote communicator |

Host software

16

Application protocol data unit (APDU)

- APDU standard

- Deploy cryptographic protocols for interchange of the messages to and from the host

17

Card keys and Locks

- Fabrication key— identifies a card uniquely
- Personalization key
- Utilization lock — used by the server to lock or unlock the use of the card

Smart Labels

- Smart Labels multiple applications in our day-to-day lives in their numerous forms such as identification Labels, key Labels, etc.

Label

- Serves the purpose of identifying the contents of a package
- A barcode label on a book packs in information about the publisher, title, author, publishing date, and reprint edition of a book
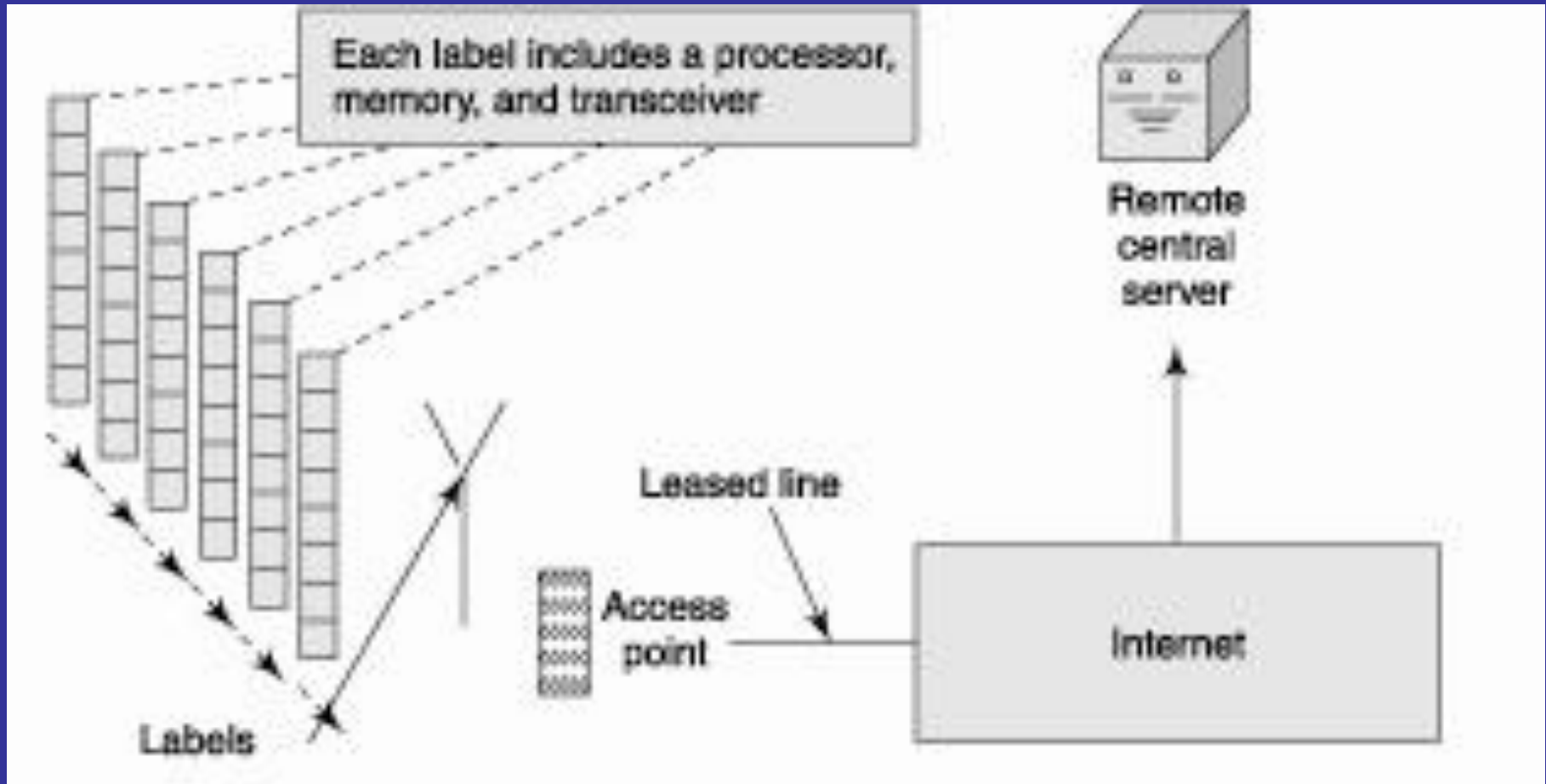
Label

- Differs from a card in terms of thickness and visibility
- A label using wireless means for product identification can be concealed inside the product

Smart Label

- Has a processor, memory, transceiver, and antenna similar to a contactless smart card
- An earlier version of the now popular RFID tags

22

Network of labels

Software in label

- Secure OS (RSA DES, ...)
- Label's data transceiver
- Collision-sense-and-avoidance protocol
- Application
- LAN
- Data aggregator
- Communicator to access point

Label software

Access point software for label

- Secure OS (RSA DES, ...)
- Host data transceiver
- Application
- LAN communicator
- Server-authentication software
- Remote central server

Access point software

Smart Labels Network

- Networked together using a central reading and computational device (host) or PC

- Cluster of labels form a network similar to a LAN network

- CSCA protocol used so that multiple labels are not allocated the same ID tag and the central server can uniquely identify each one

26

Smart Labels

- Use secured hardware and server-authentication software

- The central server also detect the removal of a labelled product or packet

27

Smart Token

- Used for authentication purposes before an action, such as granting entry into a restricted area, is initiated

Smart Token Protocols

- A smart token— an encapsulated chip including an embedded processor and a memory

- Token sizes small, usually of the order of a shirt button or a pen nib

29

Token Protocol For Communication

- Use either a wire-based protocol and communicate at 16 to 128 kbps or ASK 13.56 Mbps for contact-less communication

SUMMARY

- Smart card computer, memory and transceiver

- Contact and contactless

- IEEE standards

- ASK modulation

- JavaCard language for application development

Summary

- Smart Label computer , memory and transceiver

- Network of labels

- Hotspot

- Tokens

End of Lesson 03
Smart Systems─ Cards, Labels, and tokens